ANÁLISIS DEL NIVEL DE SEGURIDAD PRESENTE EN LOS DISPOSITIVOS QUE COMPONEN EL INTERNET DE LAS COSAS

ALEJANDRO URIBE CASTRO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CALI – VALLE DEL CAUCA
2019

ANÁLISIS DEL NIVEL DE SEGURIDAD PRESENTE EN LOS DISPOSITIVOS QUE COMPONEN EL INTERNET DE LAS COSAS

ALEJANDRO URIBE CASTRO

Monografía para optar al título de:
Especialista en Seguridad Informática

Director del proyecto:
Msc. Katerine Márceles Villalba

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CALI - COLOMBIA
2019

Nota de aceptación

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Cali,

DEDICATORIA

Dedico este trabajo primero que todo a Dios quien es mi guía y apoyo, a mi familia que me apoyó en todo momento y no permitió que desfalleciera, ellos han sido mi inspiración y mi motor para seguir con mi formación profesional.
A mis padres que me inculcaron los mejores valores y me brindaron una excelente educación.

AGRADECIMIENTOS

Expreso mis más sinceros agradecimientos a cada uno de los docentes, asesores y tutores de la UNAD que con sus conocimientos y dedicación me permitieron alcanzar este logro tan importante para mi formación personal y profesional.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

BOTNET: Red de computadores que han sido infectados por algún tipo de virus permitiendo su control remoto.

DDoS (Distributed Denial of Service): Ataque informático que consiste en realizar múltiples peticiones simultáneas de servicio a un sistema logrando inhabilitar un servidor, por agotamiento de sus recursos o por saturación de los canales.

HARDWARE: Elementos físicos que hacen parte de un sistema informático.

HOBBIES: Actividades que se realizan por gusto en el tiempo libre.

INTERNET: Red mundial de computadores conectados que comparten recursos y servicios

IoT (INTERNET OF THINGS): Internet de las cosas, dispositivos de uso cotidiano conectados a través de internet.

OWASP: Es una comunidad de internet dedicada brindar recomendaciones de manera gratuita para lograr el mejor nivel de seguridad en las aplicaciones web.

PROTOCOLO SSL: Conjuntos de normas de seguridad que permite cifrar la información.

PROTOCOLO TSL: Evolución del protocolo SSL, brinda un nivel de seguridad avanzado cifrando las comunicaciones.

SOFTWARE: Son los programas que se instalan en un computador para su funcionamiento, entre ellos el sistema operativo, la suite ofimática, entre otros.

SOFTWARE MALICIOSO: Programas desarrollados para afectar el correcto funcionamiento de un sistema informático.

TEST DE PENETRACION: Pruebas especializadas que se realizan a sistemas informáticos, páginas web, software o componentes informáticos en busca de vulnerabilidades.

INTRUSO: Persona que ingresa a un determinado lugar sin previa autorización.

VULNERABILIDADES: Debilidad o fallo de seguridad que se presenta en algún sistema informático, pagina web, software o componente informático que puede ser explotada por alguna amenaza.

RESUMEN

Con la llegada del internet las comunicaciones han cambiado, desde entonces todo se procesa más rápido y en tiempo real, las personas se han vuelto dependientes de cualquier dispositivo tecnológico que pueda conectarse al internet y cada una con diferentes necesidades; unos lo hacen por negocios, otros por estudio y otros por simplemente hobbies, sea cual sea la necesidad existe una característica muy especial que todos deben tener presente y no deben dejar pasar por alto, la seguridad.

Por tal motivo se propone realizar un análisis general de los componentes de seguridad existentes en los diferentes dispositivos que anteriormente solo observamos como un simple electrodoméstico y que hoy gracias al internet de las cosas o IoT por sus siglas en ingles brinda la posibilidad de integrar diferentes dispositivos a una red permitiendo su gestión remota.

No obstante, es importante tener en cuenta los niveles de seguridad que estos ofrecen para estar seguros de que la información no estará expuesta ya que al estar conectados a internet podrían representar una posible entrada a intrusos que solo esperan encontrar vulnerabilidades para sacar provecho de estas.

Para ponerse en contexto sobre la importancia de la seguridad en estos dispositivos se exponen varios ejemplos en donde algunos dispositivos IoT fueron vulnerados por no contar con mecanismos de seguridad adecuados y a través de ellos se perpetraron varios ataques que afectaron grandes compañías a nivel mundial.

Al final de este análisis se entregarán una serie de recomendaciones para que todas las personas tomen las precauciones necesarias para evitar ser víctimas de ataques informáticos.

Palabras claves: IoT (Internet of Things), Vulnerabilidades, intrusos.

ABSTRACT

With the arrival of the internet communications have changed, since then everything is processed faster and in real time, people have become dependent on any technological device that can change to the internet and each with different needs; What they do for business, others for study and others for simply hobbies, whatever the need, there is a very special characteristic that everyone should keep in mind and should not overlook safety.

For this reason it is proposed to carry out a general analysis of the specific safety components in the different devices that we previously only observed as a simple appliance and that today thanks to the internet of things or IoT for its initials in English it offers the possibility of integrating different devices to a red properly its remote management.

However, it is important to take into account the security levels they offer to be sure that the information will not be exposed since being connected to the Internet could represent a possible entry to intruders who only hope to find vulnerabilities to take advantage of these.

To put in context on the importance of security in these devices, several examples are presented in which some IoT devices were violated for not having adequate security mechanisms and through them several attacks that affected large companies worldwide were perpetrated.

At the end of this analysis, a series of recommendations will be delivered so that all people take the necessary precautions to avoid being victims of computer attacks.

Keywords: IoT (Internet of Things), vulnerabilities, intruders.

INTRODUCCION

Desde la creación del internet en los años 90´s la humanidad ha aprovechado esta tecnología para realizar actividades que antes eran inimaginables como por ejemplo: consultar de manera inmediata información que solo existía en libros impresos y que debían ser consultados solo en bibliotecas dependiendo de su disponibilidad, comunicarse en tiempo real y en vivo con familiares y amigos en cualquier lugar del mundo entre otras cosas.

Hoy en día esta tecnología es aprovechada para diversos fines como laborales, personales, de entretenimiento, educativos o cualquier otro fin que se pueda imaginar.

Este gran nivel de consumo no solo ha sido beneficioso para la sociedad sino también para la economía en donde las grandes empresas han visto cómo aprovecharlo al máximo y es así como empresas que prestan diferentes servicios han desarrollado múltiples dispositivos que no solo simplifican las actividades de las personas si no que crean una dependencia de conectividad constante.

Esta conectividad no solo hace referencia a dispositivos habituales como computadores de escritorio, computadores portátiles, tabletas, celulares inteligentes si no que va más allá llegando a dispositivos o electrodomésticos que antes solo eran diseñados para cumplir una función específica a ésta transformación del concepto del uso de los dispositivos se le conoce como el Internet de las cosas (IoT), en donde la mayoría de dispositivos electrónicos que se fabrican están diseñados para conectarse a internet.

Según Gartner en el año 2020 habrá aproximadamente 25.000 millones de dispositivos conectados a internet.

Es por esta razón que es importante tener en cuenta todos los detalles de estos nuevos dispositivos, la presente monografía “Análisis del nivel de seguridad presente en los dispositivos que componen el Internet de las cosas” se centra en analizar el nivel de confiabilidad que presentan estos dispositivos que actualmente se encuentran en el mercado.

El objetivo general de la monografía es analizar los niveles de seguridad presentes en los dispositivos que componen el Internet de las cosas, ya que es un conjunto de elementos que deben tener para evitar riesgos tales como: perdida de información sensible, contagio por software malicioso, entre otros.

Para ello debe evaluarse tanto métodos de comunicación como sistemas operativos y actualizaciones, dado que inicialmente solo era importante su funcionabilidad pero a raíz del aumento de las amenazas cibernéticas hoy en día el tema de seguridad es un factor determinante para cualquier dispositivo que se lance al mercado.

1. DEFINICIÓN DEL PROBLEMA

1.1. DESCRIPCIÓN

Con el auge de las tecnologías y la necesidad que tienen los grandes fabricantes de éstas de posicionarse en los primeros lugares de la economía, el desarrollo de sus productos "inteligentes" que harán más fácil la vida de las personas, como por ejemplo que la nevera que tienen en su casa sea capaz de realizar un pedido de leche por si misma al supermercado, cuando ésta ya se esté acabando o la de notificarnos que no hay hielo en el congelador, por citar dos situaciones en particular, se olvidan en algunos casos de un componente sumamente importante tanto como su diseño amigable y su funcionalidad, la seguridad.

Estos dispositivos que ahora se conectan a la red y que estarán expuestos en internet, deben contar con las medidas de seguridad mínimas para evitar que personas no autorizadas ingresen a ellos y desde allí puedan poner en riesgo nuestra seguridad digital.

Muchas personas solo ven lo práctico que es tener un hogar inteligente pero no tienen en cuenta las consecuencias que puede tener no tomar medidas de seguridad adecuadas, es tan importante el tema de la seguridad que en como lo menciona el diario The Washington Post[1], en su artículo del año 2016 titulado; The Day of the Zombie Baby Monitors: When hackers weaponized the Internet of Things, en donde millones de dispositivos conectados a internet entre ellos monitores para bebés, cámaras web de seguridad y grabadoras de video digital se infectaron con un malware llamado Mirai aprovechando un fallo de seguridad, posteriormente recibieron la orden de atacar una compañía de servicios de DNS, provocando así un Denegación de servicio (DDoS) inhabilitando sitios tan importantes como Twitter, Spotify y Paypal entre otros.

Otro claro ejemplo de los peligros de contar con dispositivos IoT sin medidas de seguridad es lo que le sucedió a una familia en Wisconsin, Estados Unidos, según lo informó el sitio, Noticias de Seguridad Informática[2], en donde intrusos por intermedio de un dispositivo accedido los sometieron a altas temperaturas y a música con un volumen muy elevado.

---

[1] the washington post. (25 de octubre de 2016). *the day of the zombie baby monitors: when hackers weaponized the internet of things*. obtenido de https://www.washingtonpost.com/opinions/the-day-of-the-zombie-baby-monitors-when-hackers-weaponized-the-internet-of-things/2016/10/25/167fdf42-9a1b-11e6-b3c9-f662adaa0048_story.html

[2] Noticias de Seguridad Informática. (25 de Septiembre de 2019). Hackean hogar inteligente; atacantes someten a la familia a altas temperaturas y a música a todo volumen. Obtenido de https://noticiasseguridad.com/hacking-incidentes/hackean-hogar-inteligente-atacantes-someten-a-la-familia-a-altas-temperaturas-y-a-musica-a-todo-volumen/?fbclid=IwAR0AcNBM3uCWw99QPpXY7RR1WJjbFZZuKUzTx1-bpCPtekZHZNmfSWqj0Ek

Según una investigación realizada por los Laboratorios de Kaspersky llamada Nuevas tendencias en el mundo de las amenazas IoT[3] del año 2018, reveló que los malware dirigidos a los dispositivos del Internet de las cosas han tenido un crecimiento bastante significativo iniciando la investigación en el año 2016 con 3.219 malware y cerrando el año 2018 con 121.588, por lo cual se concluye que los ojos de los atacantes están puestos hacia estos dispositivos, por ahora un blanco fácil para llegar a cometer diversos actos ilícitos hasta llegar a convertirse en delitos informáticos ya que al comprometer un dispositivo que contenga información personal y privada como videos o fotos íntimas podría llegar a Sextorsionar o chantajear al alguna persona a cambio de no revelar esa información intima.

Por otro lado, según lo afirman Tarquino y García[4], un 90% de los dispositivos IoT posee problemas de privacidad, mientras que un 70% no encripta los datos, lo que pone a la información que circula y se almacena en ellos, en un peligro constante ya que no poseen ningún mecanismo de protección para los datos confidenciales.

Con la gran cantidad de equipos que se proyectan se incorporarán al mundo IoT, los problemas de seguridad y privacidad serán demasiados.

Sin duda existen peligros al incorporar dispositivos domésticos al mundo de la red, pero es claro que estos dispositivos están ayudando con múltiples tareas en diferentes sectores de la humanidad, uno de ellos es en el área legal, en donde según Internet Society[5], un grupo de abogados en Estados Unidos han utilizado durante un juicio de divorcio los datos de hora y localización obtenidos de los dispositivos de peaje electrónico instalados en los vehículos para demostrar que un cónyuge engañaba al otro.

En otro juicio llevado en el año 2014, una mujer canadiense utilizó los datos de su propio dispositivo de actividad física tipo brazalete deportivo, en apoyo de su reclamo en una demanda por lesiones personales, donde establecerán que a causa de un accidente bajó considerablemente su actividad física, tomando como base su estilo de vida activo y los datos que arroja el dispositivo.

---

[3] Kaspersky Lab. (18 de Septiembre de 2018). *Nuevas tendencias en el mundo de las amenazas IoT*. Obtenido de https://securelist.lat/new-trends-in-the-world-of-iot-threats/87948/

[4] Tarquino Murgueito, D. F., & Garcia Garcia, E. S. (Julio de 2017). *Seguridad en internet de las cosas*. Obtenido de https://repositorio.escuelaing.edu.co/bitstream/001/605/1/Tarquino%20Murgueito%2C%20Daniel%20Felipe%20-%202017.pdf

[5] Internet Society. (Octubre de 2015). *La internet de las cosas - una breve reseña*. Obtenido de https://www.internetsociety.org/wp-content/uploads/2017/09/report-InternetOfThings-20160817-es-1.pdf

1.2 FORMULACIÓN DEL PROBLEMA

Este estudio monográfico busca analizar las medidas de seguridad con que cuentan actualmente estos dispositivos y dar respuesta al siguiente interrogante, ¿Cómo se podría minimizar los riesgos existentes aquellos dispositivos electrónicos conectados al internet de las cosas?

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Analizar los mecanismos y niveles de seguridad existentes en los dispositivos que conforman el Internet de las Cosas, para generar recomendaciones y estrategias para el uso seguro.

2.2. OBJETIVOS ESPECIFICOS

- Determinar si los mecanismos de seguridad existentes en los dispositivos del Internet de las cosas son los suficientemente confiables.
- Identificar los niveles de seguridad de los dispositivos del internet de las cosas.
- Identificar recomendaciones sobre los dispositivos que ya se encuentran en el mercado y en los diferentes hogares.
- Sugerir acciones o estrategias de seguridad a tomar para el uso de los dispositivos del Internet de las cosas poco seguros.

3. JUSTIFICACION

El análisis de los niveles de seguridad presente en los dispositivos del internet de las cosas es muy importante, dado que permitirá conocer acerca del estado de madurez en materia de seguridad con que cuentan actualmente estos dispositivos, pues se considera que no se tienen en cuenta este factor tan importante, debido a que si estos dispositivos no tienen los niveles de seguridad adecuados podrían colocar en riesgo el activo de información (dispositivo de hardware como la información contenida).

Entre los riesgos más representativos se encuentra el acceso no autorizado y la obtención de los datos personales registrados en el dispositivo como la identificación, contraseña, número telefónico, los cuales pueden ser usados en contra del dueño de esta información logrando cometer robos de dinero, extorsiones, plagio, entre otros y dependiendo de los dispositivos que logren acceder podrían tener acceso fotos y videos que podrían ser íntimos y el atacante podría utilizar esta información para cometer delitos.

En ese orden de ideas se identificarán los niveles de seguridad que existen actualmente en los dispositivos del internet de las cosas que permitirán tomar acciones y/o implementar controles que reduzcan los riesgos que pueden llegar hacer producidos por alguna amenaza. En consecuencia permitirá tener suficientes argumentos para determinar qué tan seguros se están fabricando estos dispositivos.

4. MARCO DE REFERENCIA

Es importante hacer un repaso a lo largo de la historia para identificar el punto de partida de este nuevo concepto que está revolucionando al mundo y sobre todo de aquellos conceptos indispensables para su desarrollo, por lo cual se verán reflejado en los siguientes apartados:

4.1. MARCO HISTÓRICO

Es difícil establecer una fecha exacta para el nacimiento del internet ya muchos afirman que el internet tuvo su nacimiento en los años 90´s, pero no hay que desconocer que desde los años 60´s se vinieron conociendo diferentes investigaciones que buscaban computadores conectados globalmente intercambiando información, la primera red que fue creada a partir de este concepto fue ARPANET. Esta fue gestada por el Departamento de Defensa de los Estados Unidos cuyo primer NODO fue creado en la Universidad de California.

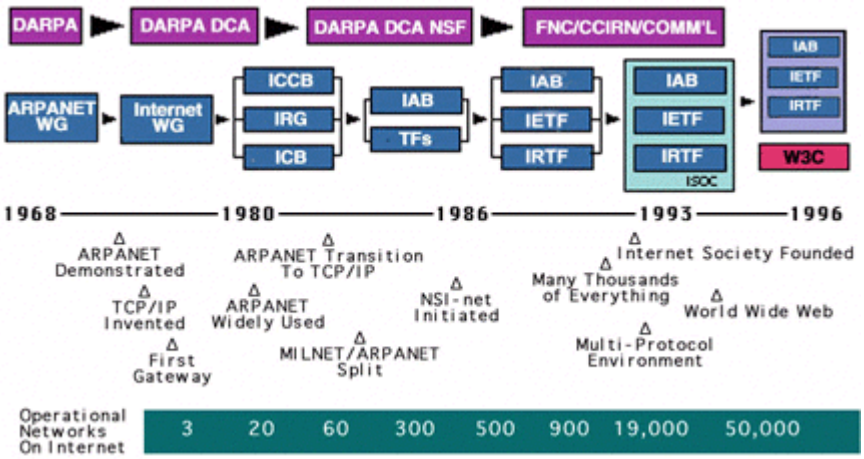
Por consiguiente en la figura 1, se puede observar la línea de tiempo de la evolución del internet desde sus inicios en el año 1968 hasta el desarrollo final cuando se llegó a conocer la red mundial www tal como funciona hoy en día.

En la primera etapa de este gran suceso comprendida entre finales de los años 60´s y 70´s la Agencia de Investigaciones de Proyectos Avanzados (ARPA) logra demostrar la conexión entre dos computadores a miles de kilómetros de distancia, unos se encontraba en Massachussetts y el otro en California mediante una línea telefónica, llamando a esta red ARPANET.

En la década de los 80´s se crea el protocolo TCP/IP esencial para la comunicación tal como se hace ahora, esto permitió ampliar la comunicación entre diferentes entidades de investigación y desarrollo pero a su vez para uso diario, el correo electrónico hacia sus primeros recorridos reduciendo el tiempo de entrega de información.

Iniciando los años 90´s se establece el concepto de interconexión a nivel mundial conocido como internet, estableciendo múltiples protocolos de comunicación, llegando a las 50.000 redes operativas.

Figura 1. Línea de tiempo evolución del internet



Fuente: https://www.internetsociety.org/es/internet/history-internet/brief-history-internet/#f3

A partir de esa fecha la evolución de la tecnología y las telecomunicaciones han sido a pasos agigantados pasando de utilizar computadores del grande de un cuarto a dispositivos que se pueden transportar con facilidad.

Según lo propuesto por el autor Medina[6], Kevin Ashton fue la persona que acuñó el término del internet de las cosas y desde sus inicios sintió la necesidad de tomarse la seguridad muy en serio.

El termino apareció en el año de 1999 cuando trabajaba para una reconocida empresa de bienes de consumo como Procter & Gamble y como la mayoría de las grandes ideas que revolucionan al mundo fue debido a una necesidad y era la de cómo resolver un problema que estaban teniendo en esa oportunidad, se invertía mucho dinero en publicidad y esto ocasionaba que los consumidores se volcaran a comprar sus productos pero desabastecían los almacenes rápidamente haciendo que los estantes lucieran vacíos, su idea fue la de colocar sensores conectados a la red para identificar cuando los productos no estaban disponibles.

En esa fecha el término “Internet para las cosas” como estuvo planteada la idea no tomó mucha fuerza debido a que en los años 90 el internet se realizaba a través de línea telefónica y era muy lento, fue en el año de 2009 aproximadamente que el término “Internet de las Cosas” se volvió mundialmente famosa.
Como lo menciona Secmotic[7] se calculó que en 2020 habrá 50.000 millones de dispositivos conectados a Internet, lo que hace una media de 6,58 aparatos por

[6] Medina, M. A. (5 de Octubre de 2017). *La historia detrás del internet de las cosas*. Obtenido de https://www.elespectador.com/tecnologia/la-historia-detras-de-la-internet-de-las-cosas-articulo-716678

[7] Secmotic. (31 de Mayo de 2016). *Internet de las cosas*. Obtenido de https://secmotic.com/internet-de-las-cosas-seguridad/

persona. Esto permitirá que prácticamente todas las funciones de los hogares, sean contralados a través de las redes, la idea que tuvo Kevin Ashton fue bien aprovechada y se le está sacando el máximo de utilidad.

4.2. MARCO CONCEPTUAL

IoT o Internet de las cosas para el autor Peña[8] es la interconexión a través de Internet de dispositivos informáticos integrados en objetos cotidianos, lo que les permite enviar y recibir datos". Con base en esto se puede deducir que ahora los electrodomésticos "dirán" que les duele o que necesitan.

Figura 2. Internet de las cosas IoT

Fuente: https://www.elespectador.com/sites/default/files/istock-638138860-1_0.jpg

En la figura 2, se puede observar el concepto que maneja el IoT en donde todos los dispositivos pueden estar interconectados a través de internet por un solo control maestro desde el cual se puede gestionar desde un bombillo hasta una lavadora o nevera.

Todos los dispositivos que se lanzan al mercado están orientados a la capacidad que tienen de conectarse a internet, en su publicación ¿Qué es el internet de las cosas? Según Rose, Eldridge, & Chapin [9], aseguran que Cisco estima que el tráfico generado por dispositivos que no son computadoras personales aumentará del 40% en 2014 a casi el 70% en 2019.

---

[8] Peña, M. (4 de Octubre de 2019). *Qué es el Internet de las Cosas y cómo afecta tu vida diaria*. Obtenido de https://es.digitaltrends.com/tendencias/que-es-el-internet-de-las-cosas/

[9] Rose, K., Eldridge, S., & Chapin, L. (8 de Septiembre de 2017). *La internet de las Cosas — Una breve reseña*. Obtenido de https://www.internetsociety.org/es/resources/doc/2015/iot-overview

Por otra parte El díario el Heraldo[10] en un artículo acerca del Internet de las Cosas se abre espacio en Colombia menciona que Cámaras de seguridad, sensores de movimiento y cerraduras inteligentes conectadas entre sí con una aplicación móvil permitirá que los usuarios tengan al alcance de su mano todo el control del sitio que desean vigilar, o en casos más simples, revisar si todo quedó bajo control, como las luces apagadas, por ejemplo. Todas estas nuevas tecnologías tendrán un único punto de control y su respuesta será en tiempo real y Colombia no está ajena a la adopción de estos beneficios.

En tiempos atrás, esto era algo que se veía muy común en las películas futuristas que las personas controlaban sus dispositivos a través de comandos de voz o centralizados en un solo control remoto, pero hoy está al alcance de muchas personas con el concepto IoT, incluso controlando sus dispositivos aun cuando no se encuentran cerca de ellos sino, a kilómetros de distancia

En resumen el IoT, es una tecnología fundamentalmente diseñada para conectar objetos cotidianos a internet, los cuales al estar conectados a internet tiene la capacidad de almacenar, gestionar e intercambiar información y lo que busca es agilizar los procesos que son realizados de manera manual convirtiéndolos en procesos automatizados.

Figura 3. Representación del internet de las cosas

Fuente: https://es.digitaltrends.com/tendencias/que-es-el-internet-de-las-cosas/

La nube tiene un papel fundamental en el IoT, ya que a través de esta se conectan los diferentes dispositivos, por lo que se puede observar en la en la figura 3, algunos de los dispositivos que son de uso cotidiano que muchas personas no se imaginarían que podrían estar conectados a internet.

[10] El Heraldo. (18 de MAyo de 2018). *El Internet de las Cosas se abre espacio en Colombia*. Obtenido de https://www.elheraldo.co/tecnologia/el-internet-de-las-cosas-se-abre-espacio-en-colombia-496312

La conexión de estos dispositivos se realizan usando protocolos de comunicación especialmente diseñados para sus procesos, otro componente importante son los sensores que se encargan de capturar la información de dispositivo para luego ser transmitida, algunos de éstos son de proximidad o movimiento, otros de temperatura y de humedad.

Sin duda estos dispositivos están en aumento y abarcando cada vez más sectores, ayudándolos a mejorar sus procesos y servicios, brindando la posibilidad de obtener información en tiempo y controlando remotamente alguno de ellos, los sectores que más se han visto beneficiado con el auge de la tecnología IoT, según Rodríguez[11] son: **Ventas, Logística, Gestión de Cadena de Suministros**, con estantes inteligentes que gestionan todo el tráfico de productos, obteniendo en tiempo real información de rotación de productos, **sector de las telecomunicaciones**, incorporando nuevos servicios como es el uso de GSM, NFC, Bluetooth de bajo consumo, WLAN, redes de múltiples saltos, GPS y sensor de redes junto con la tecnología de la tarjeta SIM, **sector salud**, permitirá significativamente una mejor medición y control de métodos de funciones vitales (temperatura, presión arterial, frecuencia cardíaca, los niveles de colesterol, glucosa en la sangre etc.) **sector de la fabricación**, permitirá obtener información acerca de todo el ciclo de vida de del producto para una mejor toma de decisión, **sector de la industria, petróleo y gas**, permitirá accionar instrumentos en locaciones difícil de acceder, no solo agilizando los tiempos de respuestas, si no preservando la vida de los trabajadores, **sector de la agricultura y ganadería**, haciendo posible la detección de tiempo real de los animales, por ejemplo durante los brotes de enfermedades contagiosas.

No obstante esta tecnología también se puede encontrar en otros sectores como lo mencionan los autores del artículo Análisis sistemático de la seguridad en internet of things[12], como por ejemplo en el: sector salud (Smart Health), sector educación (Smart Education), sector hogar (Smart home), sector transporte (Smart Transport), sector seguridad (Smart Security), entre otros; de ahí la importancia que ha tomado esta tecnología en la actualidad.

Es así, que en el mismo informe se describe la arquitectura general de IoT como se muestra en la figura 4 y por consiguiente sus amenazas como se describe a continuación:

---

[11] Rodríguez, F. G. (Abril de 2015). *El Internet de las cosas y las consideraciones de seguridad*. Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/8492/INTERNET%20DE%20LAS%20COSAS%20TESIS%20Y%20CONSIDERACIONES%20DE%20SEGURIDAD%20-%20FINAL.pdf?sequence=1&isAllowed=y

[12] Perez, N., Bustos, M., Berón, M., & Henriques, P. (Abril de 2018). *Análisis sistemático de la seguridad en internet of things.* Obtenido de http://sedici.unlp.edu.ar/bitstream/handle/10915/68387/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

Figura 4 Arquitectura general de IoT

Fuente: http://sedici.unlp.edu.ar/bitstream/handle/10915/68387/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

Capa de Percepción (CP): Realiza la recopilación de los objetos por medio de sensores que generalmente utilizan la tecnología RFID (Identificación por Radiofrecuencia), el cual presenta las siguientes amenazas:

Etiquetas: Por deficiencias en su autenticación puede presentarse acceso a las etiquetas, realizando lecturas, modificaciones o eliminaciones.

Clonación de Etiquetas: Al tener acceso a las etiquetas, podrían clonarse y esto conllevaría a que el lector no reconozca una etiqueta real o una réplica.

Spoofing: Se emite información falsa a los RFID, haciéndose pasar por la fuente original.

Capa de Red: Se encarga de la transmisión de los datos recolectados en la capa de percepción hacia cualquier red, sus principales amenazas son:

Ataque Sybil: Asignación de diferentes identidades a un mismo nodo, ocasionando información incorrecta.

Ataque de privacidad de sueño: Mantiene encendidos los nodos agotando su batería y apagándolos

Inyección de código: Inyección de código malicioso provocando control de la red.

Capa de nivel medio: Garantiza el mismo tipo de servicio entre los objetos físicos conectados, los problemas en esta capa son:

Acceso no autorizado: Eliminación de datos sensibles del sistema por parte de atacantes.

Ataque DoS: Ocasiona apagado causando indisponibilidad en los servicios.

Capa de Aplicación: Se encarga de las aplicaciones de IoT provenientes de los diferentes tipos de industrias, como por ejemplo: Smart Hospital, Smart City, Smart Transportation, entre otros. La seguridad de esta capa se encuentra afectada por:

Inyección de código malicioso: Tiene como propósito robar información.

Ataque de denegación de servicio (DoS): Engaña a la víctima haciéndole creer que el ataque real está sucediendo en otro lugar.
Ataque Spear-Phishing: Suplantación de correos electrónicos para engañar a las victimas y obtener acceso a las credenciales de esa víctima.

Características del IoT[13]
La combinación de software y hardware en la tecnología IoT proporciona la facilidad de convertir un dispositivo convencional en inteligente, mostrando las siguientes características.

- **Conectividad**: Permite compatibilidad y acceso a la red, sea cual sea el medio que le rodea.
- **Sensibilidad**: Permite la detección y el reconocimiento que reflejen un verdadero conocimiento del mundo físico y las personas.
- **Interacción:** Permite comunicación entre el mundo físico, las personas y las máquinas, productos que interactúan de forma inteligente con el mundo real.

Principales tecnologías del Internet de las Cosas[14]
Las principales tecnologías sobre las cuales se quiere impulsar el Internet de las Cosas que ayudarán en múltiples actividades y son muy importantes para el desarrollo del internet de las cosas.

- **RFID**
  "Radio Frequency Identification" (Identificación por radiofrecuencia) es una tecnología de identificación automática de objetos estáticos o dinámicos y personas, se compone de tarjetas, lectores y antenas.

- **Sensores**
  Gracias a estos se logra la recopilación de información sobre el entorno en el que se encuentran las cosas, gracias a los avances en nanotecnología, se ha logrado reducir el tamaño de los microprocesadores sin perder la velocidad de procesamiento, gracias a los sensores se obtendrá información en tiempo real y se podrá acceder a ella desde otros lugares y a través de esta información se podrán tomar decisiones remotas sobre las acciones a tomar u observar que acciones se realizaron de manera automática.

---

[13] LLerena, C. A. (Octubre de 2018). *Hacking Etico al IoT mediante SDR*. Obtenido de https://repositorio.uta.edu.ec/bitstream/123456789/28812/1/Tesis_%20t1489ec.pdf

[14] García, L. C. (2014). *Estudio del impacto técnico y económico de la transición de internet al internet de las cosas (iot) para el caso colombiano*. Obtenido de http://bdigital.unal.edu.co/50458/1/Estudio%20T%C3%A9cnico%20y%20Econ%C3%B3mico%20de%20la%20transici%C3%B3n%20de%20Internet%20al%20Internet%20de%20las%20Cosas%20%28IoT%29%20en%20el%20caso%20colombiano.pdf

- **Nanotecnología**
  Se utiliza para mejorar los productos alrededor de una serie de industrias, incluyendo los sectores de medicina, energía y el transporte. La utilización de esta tecnología hará posible que los objetos que interactúan y se conectan en la red unos con otros, sean lo más pequeños posible.

- **Tecnología inteligente**
  Son métodos empleados para lograr propósitos mediante el uso de un conocimiento a priori. Objetos que obtienen inteligencia después de la implantación de tecnologías inteligentes, se pueden comunicar con los usuarios.

En lo que concuerdan muchos expertos en materia de seguridad es que no existe un estándar para que los fabricantes de dispositivos agreguen ese toque de seguridad a sus productos, tal como lo afirma el autor del artículo de Internet de las cosas, privacidad y seguridad[15], el concepto "Security by Default" desea cambiar ese mínimo nivel de seguridad, estableciendo una configuración por defecto que sea segura en el momento de la fabricación y distribución de un dispositivo.
En el artículo se mencionan algunas debilidades de seguridad que podrian ser aprovechadas por algun atacante para vulnerar un dispositivos IoT.

Seguridad en la transmisión de datos:
Los dispositivos IoT son muy propensos a los ataques y a la obtención fácilmente información privada y personal con ataques como el conocido "Man in the Middle", el cual consiste en la interceptación de la información que viaja por los canales que no son seguros o no cifrados.

La seguridad en el software:
Muchos dispositivos se fabrican con versiones simples de Linux y Windows, entre otros, lo cual reduce los costos de fabricación pero aumenta el nivel de inseguridad de los mismos.
Si estos dispositivos que se conectan a internet no se les realiza mantenimiento, actualización y protección se convierten en un blanco fácil para ser accedido y a su vez tomar control del dispositivo y a la información allí contenida, esto podria lograrse a través de aplicaciones maliciosas alojadas en los repositorios de aplicaciones.

[15] Castro, M. (Septiembre de 2016). *Internet de las cosas. Privacidad y seguridad.* Obtenido de https://sinbad2.ujaen.es/sites/default/files/publications/Memoria_0.pdf

Seguridad en la configuración y funcionabilidad:
En muchas ocasiones el primer problema de seguridad se encuentra en la configuración que trae por defecto el dispositivo, ya que muchos fabricantes predeterminan opciones que no van a ser usadas y otras que están activas y por desconocimiento del usuario puedan emplearse mal y producir una brecha de seguridad importante.

Seguridad en el Hardware:
Los ataques contra el hardware o parte física se producen, cuando el dispositivo tiene una gran seguridad a nivel de software, cuando se encuentran en puntos aislados de la red, o cuando están bien protegidas para un acceso a través de internet.

Los ataques más frecuentes son los accesos a la información tanto volátil y no volátil como memoria RAM y discos duros. Si se puede acceder a la memoria no volátil, es posible acceder a claves, información de acceso, etc. Del mismo modo, si se puede acceder a la memoria no volátil, se puede llegar acceder a toda la información guardada.

Una manera de proteger la información ante un ataque de este tipo es el cifrado de la información.

Seguridad en los usuarios:
Los ataques de ingeniería social juegan un papel bien importante en este punto, dado que a través de ella un atacante puede obtener información privilegiada como datos de acceso, esta técnica de engaño es llevada a cabo a través de correos electrónicos fraudulentos, sitios web falsos o suplantaciones de identidad.
Lo más importante es concientizar a los usuarios a tomar las precauciones de seguridad necesarias al realizar sus actividades diarias y sobretodo que deben prestar mucha atención a cualquier situación sospechosa, ya que de nada sirve contar con todas las medias de seguridad en el dispositivo si se falla en pequeños detalles como la que puede ser el escribir la contraseña en un papel y que se deje a la vista.

5. DETERMINACIÓN DE LOS MECANISMOS DE SEGURIDAD EN LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS.

Según Rouse[16] la seguridad del internet de las cosas (IoT), es el área interesada por salvaguardar dispositivos y redes conectados en el internet de cosas. Entre las investigaciones realizadas se ha identificado que el principal problema que presentan los dispositivos conectados al internet es que dentro de su proceso de diseño no contemplan la estructura de seguridad para ellos. De ahí la importancia del análisis que se va a desarrollar para identificar si los dispositivos del Internet de las cosas, son lo suficientemente seguros.

El tema aún está por madurar, ya que así como se encuentran buenas prácticas y metodologías para realizar diversas tareas relacionadas como por ejemplo: el desarrollo de código seguro, aseguramiento de redes y sitios web; aún por el momento no existe implementación de medidas de seguridad estandarizada para el internet de las cosas. Sin embargo ya se encuentra disponible el Top Ten de OWASP para IoT, cabe anotar que OWASP es un proyecto abierto de seguridad el cual proporciona herramientas y documentación que ayuda a reducir los riesgos de las aplicaciones web y ahora del internet de las cosas.

Este Top ten OWASP[17] comprende en su orden los problemas de seguridad que están presente en el Internet de las Cosas:

1. **Contraseñas débiles, adivinables o codificadas:**
   Se presenta cuando se utilizan contraseñas fácilmente obtenibles mediante los ataques de fuerza bruta, cuando se utilizan las mismas contraseñas para todos los dispositivos o cuando incluso se utilizan las que están públicas en internet.

2. **Servicios de red inseguros (servicios de red expuestos innecesariamente):**
   Se deben evitar los servicios de red inseguros o innecesarios que se ejecutan en segundo plano y que tienen exposición a internet. A través de la explotación es posible comprometer la confidencialidad, integridad y disponibilidad de la información almacenada en el dispositivo o permitir el acceso remoto al mismo.

---

[16] Rouse, M. (Febrero de 2017). *Seguridad de internet de las cosas*. Obtenido de https://searchdatacenter.techtarget.com/es/definicion/Seguridad-de-Internet-de-las-Cosas

[17] OWASP. (4 de Octubre de 2019). *OWASP Internet of Things Project*. Obtenido de https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

3. **Interfaces inseguras del ecosistema (falta de autenticación / cifrado):**
   Herramientas como las interfaces web o servicios en la nube configurados de manera insegura, comprometen los dispositivos y los componentes que se gestionan a través éstos.
   Esta vulnerabilidad también se presenta cuando no existen controles de acceso a las interfaces mencionadas anteriormente y cuando no se encriptan las comunicaciones.

4. **Falta de mecanismo de actualización segura (falta de comprobación del firmware en el dispositivo):**
   Se presenta por la ausencia de mecanismos sencillos para realizar una actualización del dispositivo de manera sencilla y segura, medios de transmisión inseguros, ausencia de mecanismos que permitan evitar volver un paso hacia atrás y la falta de notificaciones sobre los cambios de seguridad, debido a las actualizaciones.

5. **Uso de componentes inseguros u obsoletos (Uso de componentes obsoletos o inseguros):**
   Se presenta por el uso de elementos de hardware y software poco seguros u obsoletos pueden comprometer el dispositivo. La gran mayoría de los dispositivos utilizan componentes y librerías de terceros, sistemas operativos personalizados o componentes de hardware de una cadena de suministro comprometida.

6. **Protección de privacidad insuficiente (Información personal insegura):**
   Información personal del usuario almacenada y/o gestionada en el dispositivo o en el medio al cual se conecta el dispositivo que es utilizada de manera poco segura, inapropiada o sin permiso.

7. **Transferencia y almacenamiento de datos inseguros:**
   Se presenta por falta de cifrado o controles de accesos para datos confidenciales que están dentro del ecosistema; incluyendo datos en reposo, en tránsito o durante su procesamiento.

8. **Falta de gestión de dispositivos:**
   Falta de controles de seguridad en dispositivos tales como la gestión de activos y actualizaciones, monitorización de los sistemas, políticas de desmantelamiento y borrado seguro de los dispositivos.

9. **Configuración predeterminada insegura**
   Muchos dispositivos o sistemas son lanzados con configuraciones por defecto poco seguras o sin la posibilidad de hacer más seguro al sistema mediante la aplicación de restricciones a partir de cambios en la configuración.

10. **Falta de endurecimiento físico:**
    Ausencia de medidas que permitan endurecer los dispositivos desde el punto de vista físico, lo que podría permitir ataques que lleguen a información sensible que podría ser de utilidad en un futuro ataque remoto o tomar control del dispositivo.

En este mismo orden de ideas uno de los principales factores que contribuyen a que no haya buena seguridad en estos dispositivos es que necesitarían contar con más recursos de procesamiento y memoria y hasta el momento no existe una apuesta para que un electrodoméstico cuente con estos recursos.

Como se aprecia en el marco histórico el concepto ya es lo suficientemente antiguo como para pensar que se ha debido tener un terreno ganado en materia de seguridad pero no es así, según Ferrer[18], la Comisión Europea trabaja en un reglamento de certificación de dispositivos en ciberseguridad que puede estar listo antes del final de la legislatura. Esto podría dar un respiro y daría algo para preocuparse menos, sabiendo que los dispositivos de Internet de las cosas, deben cumplir requerimientos mínimos de seguridad.

Lo anterior, podría ser el primer paso para lograr tener un nivel óptimo de seguridad pero aún falta mucho camino por recorrer ya que las grandes marcas que fabrican estos dispositivos no pertenecen a esa parte del mundo y podrían demorarse en adoptar estas medidas por lo que no estarían obligadas al inicio de esta nueva reglamentación.

Pero mientras esto ocurre muchos de estos productos son comercializados con sistemas operativos sin actualizaciones de seguridad y sin la posibilidad de cambiar sus contraseñas y si se logra hacer no obliga al usuario que aún no es consciente de la seguridad, que debe crear e implementar una contraseña segura sobre estos dispositivos.

Según lo menciona Rouse[19], la empresa de seguridad Proofpoint en el año 2013 descubrió una botnet de IoT, entre los dispositivos encontrados estaban televisores, monitores para bebe entre otros electrodomésticos.

Cualquier dispositivo que se conecte a internet es vulnerable a ataques y dependiendo de la función que cumpla puede tener acceso a información personal

[18] Ferrer, I. (26 de Octubre de 2018). *La seguridad de Internet de las Cosas precisa un cambio de comportamiento del usuario*. Obtenido de https://elpais.com/tecnologia/2018/10/26/actualidad/1540564357_433476.html

[19] Rouse, M. (Febrero de 2017). *Seguridad de internet de las cosas*. Obtenido de https://searchdatacenter.techtarget.com/es/definicion/Seguridad-de-Internet-de-las-Cosas

y confidencial que fácilmente puede ser obtenida para realizar un sin número de actividades ilícitas.

5.1. DESAFIOS DE SEGURIDAD PARA IOT

La seguridad en los dispositivos IoT enfrenta múltiples desafíos, algunos por el poco conocimiento que se tiene al respecto, para la entidad Internet Society[20], estos son los más importantes:

- **La economía no contribuye a la seguridad**
  La gran competencia que existe en el mercado obliga a los productores de dispositivos para IoT a acelerar la producción de sus artículos y para lograr un buen posicionamiento en el mercado, los costos deben ser cada vez menores, como consecuencia de esto, los fabricantes dedican menos tiempo y recursos a la seguridad.
  Una buena seguridad podría ser costosa tanto para diseñar como para implementar, alargando el tiempo de salida al mercado del producto, el aumento de estos costos se trasladarían hacia los consumidores que algunos de ellos no estarían dispuestos a asumir, haciendo que el producto no tenga aceptación comercialmente hablando.
  Por otra parte, en la actualidad son mínimas las formas creíbles y conocidas que tienen los fabricantes para comunicarles a los consumidores sobre el nivel de seguridad que ofrecen sus productos.
  Y algo para resaltar es que, el costo y el impacto de una baja seguridad recaen sobre los consumidores y no sobre los fabricantes que no sienten la responsabilidad ante un ataque que sufran sus productos.

- **La seguridad exige experiencia**
  Implementar una seguridad robusta en los dispositivos IoT requiere contar con buenos conocimientos o experiencia. Los fabricantes que se inician en el mundo del IoT pueden tener poca o ninguna experiencia con la seguridad en Internet, ya que es un concepto relativamente nuevo para algunos. Por ejemplo, un fabricante sabe perfectamente cómo hacer que un refrigerador sea seguro para su función principal y utilizar los mejores componentes físicos que existan, pero puede no comprender la seguridad en Internet. Por consiguiente, es posible que no comprenda el impacto que podría tener si su refrigerador inteligente es comprometido.

[20] Internet Society. (17 de Abril de 2018). *Seguridad de la IoT para formuladores de políticas*. Obtenido de https://www.internetsociety.org/es/resources/2018/iot-security-for-policymakers/#_ftn18

- **Los sistemas de la IoT son complejos y todo su ecosistema debe ser seguro**
  En los sistemas IoT, puede que diferentes componentes estén bajo el control de múltiples participantes con diversas autoridades (por ejemplo, un servidor puede estar ubicado en un país, mientras que el dispositivo IoT puede ser fabricado en otro y utilizado en un tercer país), lo que dificulta una regulación en conjunto para los que participan en el desarrollo de todas las partes del dispositivos IoT y de esta manera minimizar los problemas de seguridad.

- **Debe mantenerse el soporte de la seguridad**
  Todos los componentes de los dispositivos IoT, tales como el sistema operativo, aplicaciones y servicios, eventualmente requieren parches de seguridad y actualizaciones para minimizar el riesgo de una explotación de vulnerabilidades conocidas. En muchos casos, los consumidores no poseen los conocimientos necesarios para implementar estos parches o actualizaciones de seguridad, por otro lado, algunos de los dispositivos no incorporan interfaces de usuario amigables que permitan interactuar de manera sencilla. Para complicar aún más las cosas, cuando se cuenta con la opción de actualizar, ésta no es obligatoria, permitiendo decidir al usuario si parcha su dispositivo.

- **Los consumidores saben poco o nada sobre la seguridad**
  En general, los conocimientos que tienen gran parte de los consumidores sobre la seguridad de los dispositivos IoT es limitado o en algunos casos nulo, lo que ocasiona que no sea un requisito a la hora de adquirir un dispositivo IoT. Muchos consumidores suelen tener limitaciones en su presupuesto, por lo que sensibilizar y educar a los consumidores son desafíos particularmente importantes.

- **Para los consumidores puede ser difícil identificar o manejar un incidente de seguridad**
  Si bien es cierto que los consumidores tienen pocos conocimientos en seguridad, lograr identificar que algo está ocurriendo con su dispositivo parece casi imposible, ya que, en muchos de los ataques, los dispositivos comprometidos siguen funcionando de manera normal sin alertar al propietario, esto hace que sea un ataque perfecto, porque mientras cumpla su función principal el dispositivo no despertará ninguna sospecha y éste a su vez puede ser parte de una botnet realizando ataques DDoS o enviando la información que logre capturar.

- **Los mecanismos de responsabilidad legal existentes pueden ser ineficientes**
  Aun no es clara la responsabilidad que tienen las partes ante una falta de seguridad adecuada, es difícil precisar si el fabricante es responsable de no

implementar los controles adecuados, o de comunicarle al consumidor cuales posee el dispositivo o si por el contrario el consumidor es el responsable por no exigirlos o no estar atento a sus actualizaciones o parches de seguridad. Esto genera incertidumbre entre las víctimas de ataques a la hora de asignar responsabilidades u obtener una compensación por los daños sufridos.

5.2. TIPOS DE RIESGOS EN LA SEGURIDAD IOT

Los riesgos informáticos están a la vuelta de la esquina para este tipo de dispositivos conectados a la red de internet, a continuación se listarán los riesgos a los cuales están expuestos según Merella[21]

- **Ataques informáticos:** Por encontrarse en un entorno de nube estos son la amenaza más común que pueda existir, entre ellos se encuentran, denegación de servicio, malware, exploits, violación de privacidad y alteración de los componentes.

- **Vulnerabilidades de Software:** Es un aspecto que se descuida mucho ya que no son actualizados constantemente y no se analizan.

- **Intercepción de datos:** Capturas de información por no contar con protocolos de información que cifren los datos.

Teniendo en cuenta los riesgos anteriormente mencionados, es importante mencionar las amenazas que acechan los dispositivos IoT, las cuales según Sigfox[22]provienen de tres fuentes:

- **Hacks de red**

  Los hacks de red ocurren cuando los dispositivos se ven comprometidos a través de la red a la que están conectados, de tal forma que al atacante le permite obtener el control del dispositivo y manipularlo como desee. Por ejemplo, el atacante podría aprovechar un dispositivo en un automovil para controlar su conducción y provocar un choque, o un termostato para controlar la temperatura de un horno industrial y causar daños a una fábrica.

[21] Merella, A. (7 de Marzo de 2018). *Seguridad Informática en dispositivos Iot*. Obtenido de https://apiumhub.com/es/tech-blog-barcelona/seguridad-informatica-en-dispositivos-iot/

[22] Sigfox. (28 de Agosto de 2019). *Seguridad de IoT: amenazas actuales y cómo superarlas @Sigfox*. Obtenido de https://www.wndgroup.io/2019/08/28/seguridad-de-iot-amenazas-actuales-y-como-superarlas-sigfox/

- **Ataques Distribuidos de Denegación de servicios (DDoS)**

  Los ataques DDoS ocurren cuando los dispositivos se manipulan para enviar tantos mensajes que la red de IoT se satura, colapsa y se inhabilitan los servidores. Los atacantes usan estos ataques para tomar el control de múltiples dispositivos comprometidos para crear un bloqueo completo, evitando que la información necesaria llegue a su destino.

- **Bloqueo de Radiofrecuencia**

  Los dispositivos IoT inalámbricos, como por ejemplo las alarmas de seguridad, pueden bloquearse mediante la interferencia deliberada con las comunicaciones inalámbricas. Este proceso se realiza mediante la adquisición de un dispositivo de interferencia de Radiofrecuencia ilegal, el cual es capaz de hacer que los dispositivos IoT pierdan conectividad, limitando su comunicación con la red, permitiendo realizar robos al no permitir que las alarmas se comuniquen con el proveedor de seguridad.

No obstante, cualquier tipo de dispositivo IoT están siendo un blanco muy apetecido, debido que a través de ellos se pueden recolectar información personal, financiera, educativa, medica que puede servirle a un ciberatacante para dirigir perpetrar su ataque de manera que no se tenga tiempo de reaccionar, cabe recordar que los ciberdelincuentes no siempre están solos, en muchas ocasiones son un grupo de personas que se valen de cualquier método para cumplir su cometido sin importar cuál sea el plano, sea éste plano virtual o físico.

Por otro lado existen otros riesgos asociados a los dispositivos IoT que son abordados por CSIRT-CV[23] (Centro de Seguridad TIC de la comunidad Valenciana), que centra su análisis en las amenazas que están expuestos los dispositivos que podrían llegar a afectar la **accesibilidad** del dispositivo, la **integridad** de la información que contiene, la **disponibilidad** es quizá el que más problemas genera, ya que; por ejemplo en el sector industrial un ataque de DDoS puede producir grandes pérdidas, la **confidencialidad** de los datos que son almacenados en los dispositivos o transmitidos a través del internet y la **identidad** del usuario o propietario, siendo esta la más grave ya que podría provocar una suplantación de identidad.

En el artículo se describen ejemplos bastante prácticos y cotidianos acerca de los riesgos que se mencionaron anteriormente:

[23] Centro de Seguridad TIC de la Comunitat Valenciana. (s.f.). *Seguridad en Internet de las Cosas, Estado del arte*. Obtenido de http://www.csirtcv.gva.es/sites/all/files/downloads/%5BCSIRT-CV%5D%20Informe-Internet_de_las_Cosas.pdf

- **Localización a través del GPS (Global Positioning System)**
  En la actualidad existen muchos artículos de uso frecuente que se utilizan para supervisar cualquier actividad, siendo la deportiva la que más se busca monitorear, es por esto que muchas personas utilizan los dispositivos llamadas wareables, los cuales son dispositivos que se llevan puesto para controlar o arrojar la información que deseamos acerca de la actividad desarrollada, un ejemplo de estos dispositivos son; relojes inteligentes, gafas inteligentes, ropa tecnológica, pulseras electrónicas, etc.
  Por lo general, estos van conectados a internet y traen consigo un GPS que permite ubicar geográficamente al usuario que porte estos dispositivos y esta información se aloja en algún sitio web y de acuerdo a la configuración de la privacidad podría ser accedida por cualquier persona.
  De igual manera se debe tener presente que aplicaciones en segundo plano utilizan la geolocalización de los teléfonos inteligentes.
  El riesgo que conlleva esta información en poder de desconocidos radicaría en que se conozcan los recorridos habituales que se realizan y la utilicen para cometer algún delito contra esa persona.

- **Robo de información**
  Cada vez más en los dispositivos que se conectan a internet se almacenan mucha más información, incluso hasta información sensible, en muchos casos se puede acceder a esta información a través de otros dispositivos conectados a internet, o desde entornos web o aplicaciones móviles donde se accede a través de un usuario y una contraseña.
  En caso de que un tercero lograra acceder, tendría acceso a toda esa información que podría incluso vulnerar la privacidad de las personas.
  Pero no en todos los casos el robo de información obedece a falta de controles de acceso, ya que muchos dispositivos tienen un tamaño muy reducido que facilita la pérdida de estos, pudiendo ser encontrados por cualquier persona y por ende tener acceso a la información.

- **Control y uso malintencionado de los dispositivos**
  Uno de los riesgos más frecuentes son los ataques que tienen como objetivo el control remoto de los dispositivos IoT.
  De esta forma podrían controlar remotamente y realizar toda clase de acciones como por ejemplo: en neveras, hornos, lavadoras o incluso automóviles.
  Dependiendo del dispositivo controlado remotamente se puede ver comprometida la integridad física de los usuarios.
  Aunque muchos de los ataques se realizan a entornos personales y domésticos, hay entornos que son para considerar, los llamados: **SCADA** (Supervisory Control And Data Acquisition; Supervisión, Control y Adquisición de Datos), que se encargan de controlar y supervisar procesos industriales a distancia, entre ellos se encuentran sistemas de control de

tráfico, sistemas de transporte o sistemas de distribución de agua entre otros, que utilizan sensores inteligentes para gestionar todos sus procesos, sería muy riesgoso que se produjera un ataque que comprometa alguno de estos sistemas tan importantes.

Tomando como base en el estudio "Análisis y parametrización de la seguridad en sistemas IoT"[24], se describen unas nuevas series de amenazas que son agrupadas en diferentes grupos en función de la finalidad para la cual se utilizan.

- **Grupo 1. Abusos/Ataques**
  Se encuentran las amenazas que buscan controlar el dispositivo, entre las cuales se encuentran: los malware, Exploit, ataques de Denegación de Servicios y ataques dirigidos.

- **Grupo 2. Interceptores/Secuestradores de comunicaciones**
  Amenazas que se utilizan para recolectar información de los dispositivos mientras es transferida a través de redes inseguras, entre los cuales se encuentran los ataques de Hombre en el Medio, el cual intercepta las comunicaciones, teniendo la posibilidad de manipular la información.

- **Grupo 3. Caídas**
  Surgen tras dejar de funcionar alguna de las partes de la red IoT, entre las cuales se tienen: caídas de red, fallo de los dispositivos y fallas del sistema.

- **Grupo 4. Empleados maliciosos**
  Surgen tras exponerse datos sensibles intencionadamente, como por ejemplo: la fuga de información.

- **Grupo 5. Desastres**
  Amenazas relacionadas con desastres naturales, tales como: terremotos, inundaciones que afecten físicamente los dispositivos.

- **Grupo 6. Ataques físicos**
  Amenazas relacionada con la destrucción de los dispositivos, ya sea por vandalismo o robo.

- **Grupo 7. Efectos inintencionados**
  Amenazas presentadas por una mala praxis involuntaria, tales como: falta de profesionales expertos en la manipulación de los dispositivos.

[24] Bartual, Ó. P. (2018). *Análisis y parametrización de la seguridad en sistemas IoT*. Obtenido de https://riunet.upv.es/bitstream/handle/10251/106950/PERERA%20-%20An%C3%A1lisis%20y%20parametrizaci%C3%B3n%20de%20la%20seguridad%20en%20sistemas%20IoT.pdf?sequence=1&isAllowed=y

5.3. ANTECEDENTES DE SEGURIDAD PARA IOT

Sin duda ataques informáticos se presentan todos los días, en su mayoría hacia grandes compañías alrededor del mundo, algunos buscando algún tipo de lucro y otro solo generando caos y daños que causan pérdidas de dinero.

Ataques como el Ransomware (secuestro de información) se escucha en todo el mundo, pero aunque parezca poco creíble ataques a monitores para bebés conectados a internet han causado grandes consecuencias.

El ataque más grande hacia dispositivos IoT como se mencionó anteriormente se presentó en el año 2016 en donde millones de dispositivos que perecen inofensivos y prestan un gran servicio a miles de personas como los son los monitores para bebés provocaron una caída de los servicios de grandes compañías en los Estados Unidos, ocasionando no solo pérdidas económicas si no reputacionales.
En el año 2013 un investigador de la firma Proofpoint[25] descubrió que en una campaña de envío masivo de correos electrónicos o Spam, alrededor de 7.500.000 de esos correos provenían de dispositivos diferentes a computadores, entre ellos routers, centros multimedia, televisores y hasta una nevera.

Otro caso muy sonado por la magnitud del ataque fue la ocurrida en el año 2018, según el Diario El Mundo de España[26], un atacante a través de un termómetro ubicado en una pecera logró sustraer una base de datos de un importante casino de un hotel en Londres.

No obstante, otro de los casos relevantes fue el de la pecera que utiliza el termómetro conectado a internet para regular la temperatura de ellas y alertar cualquier anomalía en su temperatura, el robo no incluyó dinero del casino si no información sensible de los clientes que luego fue subida a la nube.

El atacante aprovechó una debilidad en los mecanismos de seguridad del dispositivo y a través de él tuvo su ingreso a la base de datos.

Pero sin duda un caso muy publicitado fue el hackeo que realizaron unos atacantes chinos a un auto de la marca Telsa que consistió controlar a distancia el cierre de

[25] Proofpoint. (16 de Enero de 2014). *Your Fridge is Full of SPAM: Proof of An IoT-driven Attack*. Obtenido de https://www.proofpoint.com/us/threat-insight/post/Your-Fridge-is-Full-of-SPAM

[26] El Mundo. (17 de Abril de 2018). *Un hacker roba en un casino colándose a través de una pecera*. Obtenido de https://www.elmundo.es/tecnologia/2018/04/17/5ad4a14c46163f1f658b4630.html

las puertas y las luces según el artículo de El Confidencial[27], esto generó muchos comentarios negativos ya que otra vulnerabilidad explotada podrían afectar la seguridad física de los usuarios si se viera comprometido el sistema de frenos o el arranque del vehículo.

Pero estos son solo tres casos de ataques a dispositivos del internet de las cosas, que involucra un termómetro, una nevera y hasta un vehículo como principales objetivos.

Según lo afirma el portal My Seguridad[28], en un reciente estudio desarrollado por la empresa de ciberseguridad de Israel SAM Seamless Network, **las cámaras de seguridad** son los dispositivos más atacados recibiendo un 47% de los ataques realizados en las redes domésticas, estos ataques son efectuados como consecuencia de la baja seguridad de los modelos más económicos. Además, muchos de los modelos de cámaras de seguridad se basan en los mismos planos y esquemas, lo que conlleva a que, si un modelo presenta un problema de seguridad, este problema esté presente en los demás modelos.

En segundo lugar se encuentran los **hubs inteligentes** con un 15% de ataques, seguidos de impresoras, Smart tv´s y los teléfonos IP, el principal problema de seguridad que presenta este tipo de dispositivos radica en la poca seguridad que traen de fábrica, otro problema de seguridad es que cuentan con contraseñas de acceso bastante sencillas, y que además no pueden cambiarse. Es así, en el caso de que sí permitan su cambio, la necesidad de cambiar la contraseña suele pasar desapercibida de cara a sus propietarios ya que es opcional, facilitando el acceso de los atacantes a las redes a las que se conectan.

Los ataques son realizados en su mayoría en horas de la noche, aprovechando el descanso de los propietarios y de esta manera pasar desapercibido. Estos ataques se presentan en un promedio de 5 al día.

Por otra parte el portal SignalsIot[29], sitio web enfocado en Internet de las Cosas y tecnologías relacionadas para los mercados de América Latina y el Caribe, afirma que para el primer semestre de este año en el mundo se produjeron 105 millones de ataques provenientes de 276.000 direcciones IP, destacando en su artículo los

---

[27] El Confidencial. (21 de Julio de 2014). *'Hackers' chinos logran vulnerar la seguridad del coche Tesla*. Obtenido de https://www.elconfidencial.com/tecnologia/2014-07-21/hackers-chinos-logran-vulnerar-la-seguridad-del-coche-tesla_165313/

[28] Muy Seguridad. (2019). Estos son los dispositivos IoT más atacados por los hackers. Obtenido de: https://www.muyseguridad.net/2019/06/13/estos-son-los-dispositivos-iot-mas-atacados-por-los-hackers/

[29] Signals IoT. (18 de Octubre de 2019). *Según estudio, Brasil es el segundo país con más ataques a dispositivos IoT*. Obtenido de https://signalsiot.com/segun-estudio-brasil-es-el-segundo-pais-con-mas-ataques-a-dispositivos-iot/

países que más ataque sufren en el mundo, ubicando a China con el 30% de los ataques, seguido por Brasil con el 19% y Egipto con el 12%.

En su gran mayoría estos ataques fueron de fuerza bruta que busca vulnerar las contraseñas que sea débiles, en muchos de los casos las contraseñas se dejan por default, facilitando la labor de los atacantes, entre los inicio de sesión más comunes se encuentran, support / support, admin / admin o default / default, por lo que la primera recomendación que se realiza es cambiar inmediatamente las contraseñas de inicio por defecto.

Sin duda uno de los más recientes ataques fue el descubierto por Microsoft[30], el cual afirma que detectó un hackeo de aproximadamente 1.400 dispositivos IoT, el ataque se produjo por un grupo de hackers ruso llamado "Strontium", vulnerando dispositivos de organizaciones políticas, organizaciones de gobierno y ONG´s.

Los dispositivos vulnerados fueron una impresora, un teléfono de voz con IP y un decodificador de video, el común denominador de estos dispositivos que permitieron el ataque, fueron las contraseñas por defecto que seguían presentes y la falta de actualizaciones.

5.4. MECANISMOS DE SEGURIDAD PARA IOT

Con base en lo anterior se observa que ninguna empresa u hogar está exenta de sufrir algún ataque informático que vulnere su seguridad y comprometa el correcto funcionamiento del dispositivo y más grave aún, la información que procese o almacene.

El tema de la seguridad en el internet de las cosas cada día preocupa más a las empresas y en especial a los grandes países, como lo menciona Diario TI, en su artículo titulado: La necesidad de seguridad en los dispositivos iot[31], Estados Unidos en el año 2017 propuso un proyecto de ley que busca que los dispositivos IoT adquiridos por ese gobierno deben cumplir ciertos requisitos o mecanismos de seguridad.
La ley llamada "*The Internet of Things (IoT) Cybersecurity Improvement Act*"[32] busca que los fabricantes no solo garanticen la calidad de sus productos y la

[30] Melian, E. (12 de Agosto de 2019). *Microsoft detecta un hackeo masivo en dispositivos con IoT*. Obtenido de https://www.ciberseguridadpyme.es/destacado/microsoft-hackeo-iot/?cn-reloaded=1

[31] Diario TI. (06 de 02 de 2018). *La necesidad de seguridad en los dispositivos iot*. Obtenido de https://diarioti.com/opinion-la-necesidad-de-seguridad-en-los-dispositivos-iot/106732

[32] Warner, M. (11 de Marzo de 2019). *Bipartisan Legislation to Improve Cybersecurity of Internet-of-Things Devices Introduced in Senate & House*. Obtenido de https://www.warner.senate.gov/public/index.cfm/2019/3/bipartisan-legislation-to-improve-cybersecurity-of-internet-of-things-devices-introduced-in-senate-house

competitividad de sus precios sino que integren mecanismos de seguridad que garanticen que estos dispositivos sean menos vulnerables a ataques informáticos. Esta ley integraría al Instituto Nacional de Estándares y Tecnología (NIST) para que determine cuáles serían esos mecanismos de seguridad que deben optar esos dispositivos tales como: Desarrollo seguro, administración de identidades, actualizaciones de seguridad y la administración de la configuración.

Dos años después del artículo del Diario TI, esta ley aún se encuentra en proceso de aprobación lo que indica que a pesar de existir la necesidad de regular estos dispositivos falta tiempo para lograr una reglamentación adecuada que permita contar con dispositivos más seguros.

Tomando como base el informe de seguridad de Centro de Seguridad TIC de la Comunitat Valenciana, titulado: Seguridad en Internet de las cosas, Estado del arte[33], en el cual se analizan los mecanismos de seguridad existentes en los dispositivos del internet de las cosas se concluye lo siguiente:

Comunicaciones poco seguras:
Una de las funciones principales de los dispositivos del IoT es la transferencia de información; sin embargo no toda esta información viaja segur, dado que no existe el ciframiento del canal en la mayoría de las casos por donde se transmite la información, esto podría ser aprovechado por algún hacker que interfiera esta información y obtenga por medio de una ataque denominado Man In The Middle[34], (el cual consiste en interceptar información a través de canales no cifrados), información privada y confidencial de la víctima.

Sistema Operativo:
Otro mecanismo de seguridad poco seguro hasta el momento es el Sistema Operativo, en virtud de que estos dispositivos no cuentan con un parcheo automático de su software, en muchos casos no existen actualizaciones ni tampoco cuentan con una solución de antivirus para evitar ser contagiados de algún malware que sea descargado o introducido accidentalmente a través de algún medio de almacenamiento extraíble como lo son las memorias USB para el caso de los Smart Tv que cuentan con este tipo de puertos adicionales. Si bien es cierto que un software bien parchado puede representar un alto nivel de seguridad ya que no presenta vulnerabilidades, muchos fabricantes pasan por alto este aspecto ya que

---

[33] Centro de Seguridad TIC de la Comunitat Valenciana. (s.f.). *Seguridad en Internet de las Cosas, Estado del arte*. Obtenido de http://www.csirtcv.gva.es/sites/all/files/downloads/%5BCSIRT-CV%5D%20Informe-Internet_de_las_Cosas.pdf

[34] Kaspersky Lab. (10 de Abril de 2013). *¿Qué Es Un Ataque Man-In-The-Middle?* Obtenido de https://latam.kaspersky.com/blog/que-es-un-ataque-man-in-the-middle/469/

no pretenden que el usuario destine algún tiempo esperando que su dispositivo se actualice sin tener la posibilidad de usarlo.

Autenticación:
Muchos de los dispositivos IoT cuentan con un mecanismo de seguridad fundamental para evitar que personas no autorizadas tomen control o accedan a ellos, una contraseña. Este es sin duda un mecanismo con el que algunos se sienten tranquilos, ya que solo la contraseña es conocida por las personas que acceden a los dispositivos.

El problema radica en que algunos dispositivos IoT no establecen los controles necesarios para garantizar que esas contraseñas sean seguras y difíciles de descifrar, muchos de estos dispositivos no cuentan con parámetros de seguridad como la longitud y la complejidad de las contraseñas, entre más larga sea una contraseña y se combine con caracteres alfanuméricos y caracteres especiales será mucho más difícil de ser revelada.

El doble factor de autenticación no está presente en muchos dispositivos IoT ni tampoco el servicio de alertas para inicios de sesión desde diferentes dispositivos.

Firmware:
El firmware es un intercomunicador entre los componentes físicos y lógicos de un dispositivo inteligente de ahí su importancia.

Muchos de los ataques van dirigidos hacia estos programas, por lo que controlan las funciones básicas de un dispositivo y sus actualizaciones aunque corrigen fallos de seguridad, éstas deben realizarse de forma manual, lo que perjudica considerablemente su nivel de seguridad, dado que se debe tener mucho cuidado al realizar una actualización, debido a un mal proceso podría dejar sin funcionamiento el dispositivo, por esta razón no es muy común tener un firmware actualizado.

Culturización:
Para muchos este no podrá ser considerado un mecanismo de defensa de los dispositivos IoT, pero resulta ser fundamental, por lo que a través de los usuarios se realizan los parámetros de seguridad iniciales, dispositivos como Routers, Access Point, cámaras IP ofrecen medidas de seguridad que en muchas ocasiones el usuario omite ya sea por desconocimiento o por no considerarlo importante y no realiza cambios en su configuración inicial dejando contraseñas por defecto que fácilmente son descubiertas por los atacantes ya que es el primer paso que realizan los hackers cuando desean vulnerar un sistema o un dispositivo; la contraseña por defecto.

En otras ocasiones los atacantes utilizan la ingeniería social para obtener la información necesaria para cometer sus propósitos, como lo son: las credenciales de acceso a los dispositivos solo empleando sus habilidades de convencimiento, se ganan la confianza de la víctima y ésta fácilmente proporciona sin darse cuenta las credenciales de acceso.

La seguridad en los dispositivos del Internet del cosas debe ser un tema que no se puede tomar a la ligera y es muy importante que desde su diseño y posterior fabricación esté contemplado por parte de los desarrolladores, si bien es cierto que actualmente existen unos mecanismos mínimos de seguridad en estos dispositivos IoT, no son los suficientemente confiables ya que en cada uno de ellos presentan debilidades que deben ser corregidas o ajustadas para garantizar un nivel apropiado de seguridad, evitando así los accesos no autorizados, la manipulación remota de ellos y porque acciones delictivas cometidas a través de estos dispositivos.

6. IDENTIFICACIÓN DE LOS NIVELES DE SEGURIDAD DE LOS DISPOSITIVOS DEL IOT

Los dispositivos que ahora hacen parte del mundo IoT en su gran mayoría han sido diseñados inicialmente para cumplir funciones específicas, como por ejemplo una lavadora para limpiar la ropa, una nevera para conservar los alimentos a cierta temperatura, cámaras de vigilancia para observar lo que ocurre alrededor, entre otros, pero con la llegada del internet, cada uno de estos dispositivos fue incorporando componentes adicionales que les permiten transferir o almacenar información para su consulta sin importar el lugar donde se encuentre quien tenga autorización para acceder a ella.

A continuación se detallan los niveles de seguridad[35] que se han incorporado en los dispositivos IoT, en consecuencia de la necesidad de ir asegurando por completo el dispositivo, cabe anotar que aun cuando se desglosan por niveles la seguridad de estos dispositivos, en alguno de estos niveles, se presentan deficiencias en su seguridad.

Nivel de Seguridad del software:
Sin duda es el nivel más atacado, ya que a través de este se puede tener acceso a todas las opciones del dispositivo.

Uno de los dispositivos IoT más comercializados son los televisores inteligentes o Smart Tv, algunos de estos cuentan con sistemas operativos propios o adaptaciones de los existentes, entre los sistemas operativos que son utilizados en las diferentes marcas según Adslzone[36], se encuentran los siguientes:

- **Android TV:** Hisense, Philips, Sharp, Sony, Toshiba, entre otros
- **Firefox OS (ahora My Home Screen 2.0):** Panasonic
- **Roku TV:** Hisense USA, Hitachi, RCA, Sharp USA, Philips USA
- **Tizen OS:** Samsung
- **WebOS:** LG

Las actualizaciones en estos sistemas operativos no son tan frecuentes a diferencia de los sistemas operativos de los computadores o Smartphone, lo que da pie a la convivencia con vulnerabilidades que puedan ser explotadas.

---

[35] Centro de Seguridad TIC de la Comunitat Valenciana. (s.f.). *Seguridad en Internet de las Cosas, Estado del arte*. Obtenido de http://www.csirtcv.gva.es/sites/all/files/downloads/%5BCSIRT-CV%5D%20Informe-Internet_de_las_Cosas.pdf

[36] Adsl Zone. (24 de Noviembre de 2017). *¿Qué sistema operativo lleva cada marca de Smart TV?* Obtenido de https://www.adslzone.net/2017/11/24/smart-tv-fabricantes-marcas-sistema-operativo/

Por otro lado está el hecho que no en todos los casos las actualizaciones que liberan los fabricantes son informadas al consumidor como prioritaria, por el contrario se deja a consideración de ellos, como el consumidor no tiene en su conciencia la importancia de la seguridad, no se realiza por el temor de que dicha actualización modifique algo del funcionamiento y el dispositivo presente fallos posteriores a la instalación de las actualizaciones.

Como si fuera poco lo anterior, los consumidores, algunos por el simple hecho de querer estar a la vanguardia de la tecnología descargan e instalan aplicaciones que no son propias del fabricante para obtener algunas funcionalidades extras y que se adquieren de sitios externos, lo que coloca en peligro la seguridad del sistema operativo, ya que este no realiza ninguna validación de seguridad que advierta que la aplicación que está a punto de instalar podría poner en peligro todo el sistema operativo.

Las interfaces web que traen consigo estos dispositivos son muy atacados ya que como lo menciona la CSIRT[35], son de tamaño reducido y como no disponen de periféricos, tales como monitores, teclados, mouses, su administración se realiza desde otros dispositivos a través de publicaciones en internet para facilitar su gestión.

En muchos de los casos al utilizar plataformas web comunes, cuando se identifican vulnerabilidades de seguridad, estas afectarán a todos los dispositivos que las incorporen.

Para mitigar un poco la vulnerabilidad que tiene el sistema operativo en alguno de los dispositivos IoT como los Smart TV, empresas de seguridad como McAfee y ESET, según el diario la Vanguardia[37], tienen disponibles soluciones de seguridad para la protección de este tipo de televisores inteligentes, la solución de ESET, llamada ESET SmartTV Security ofrece una solución Antivirus, Anti-Ransomware, Anti-Phishing y Análisis USB en tiempo real, con lo cual, buscan garantizar la seguridad en todos los frentes posibles que podrían afectar el sistema operativo.

Nivel de Seguridad en la transmisión de datos:
En este apartado se encuentra la seguridad que ofrecen los dispositivos IoT al momento en que la información viaja a través de internet.

[37] La Vanguardia. (19 de Junio de 2019). *¿Es necesario usar un antivirus en un televisor inteligente?* Obtenido de https://www.lavanguardia.com/tecnologia/20190619/462958797967/smart-tv-antivirus-seguridad-televisor-malware.html

La transmisión de la información se realiza a través de redes cableadas o redes inalámbricas, estas últimas son las más susceptibles a recibir ataques sobre todos cuando se trata de redes inalámbricas públicas.

Si no existiera la seguridad a nivel de transmisión de datos, la información podría verse comprometida por ataques tales como el "Man in the Middle", que consiste en la interceptación del tráfico entre el emisor y receptor de la información.

Es importante tener en cuenta que cuando se navega en internet en los diferentes sitios web y más aún cuando se realiza a través de alguno de los dispositivos IoT que permitan esas interfaces web, siempre observar que el sitio cuente con un certificado de seguridad SSL que garantiza que la comunicación se cifra y de esta manera se evita una interceptación de cualquiera que sea la información que se transmita.

Por otro lado Isaca[38], afirma que el protocolo TCP, el cual es el protocolo de control de transmisión por sus siglas en inglés, Organizaciones como Microsoft, IBM y Allegro, lo han mejorado y de allí se desprenden las siguientes mejoras:

- **Message Queuing Telemetry Transport (MQTT)**
  Un protocolo basado en TCP que admite la autenticación del dispositivo, encriptación SSL (Secure Sockets Layer), seguridad en la capa de transporte (TLS).
- **Constrained Application Protocol (CoAP)**
  Protocolo de transporte basado en protocolo de datagramas de usuario (UDP), soporta micro dispositivos y tiene una huella mucho menor que HTTP. Soporta cifrado Advanced Encryption Standard (AES).

Nivel de Seguridad del hardware:
Es el nivel menos atacado según CSIRTCV[35], pero es sin duda la que presenta una alta criticidad y es mucho más difícil de subsanar ya que se compromete todo el dispositivo como tal.

El nivel de seguridad depende en gran medida de lo crítico que sea el dispositivo para el fabricante, el uso que se le vaya a dar y la criticidad de los datos que gestione.

[38] Patel, H. (2017). *IoT necesita una mejor seguridad*. Obtenido de https://www.isaca.org/Journal/archives/2017/Volume-3/Pages/iot-needs-better-security-spanish.aspx?utm_referrer=

No obstante, empresas como Microchip Technology Inc. Que según Interempresas[39] han concentrado sus esfuerzos en la seguridad basada en hardware como única forma de proteger credenciales para hacerle frente a ataques físicos o extracciones remotas. Su desarrollo ha significado tiempo en desarrollo y costos en configuraciones.

El producto desarrollado por esta compañía, el Trust Plataform ofrece almacenamiento seguro para fabricantes de cualquier tamaño, que deseen implementar de manera fácil una autenticación segura.

Dentro de su gama de productos para la seguridad de hardware ofrece tres soluciones llamadas Trust&GO, TrustFlexv y TrustCustom cada una con elementos seguros preinstalados, preconfigurados o totalmente personalizables y listos para usar, permitiendo así que los desarrolladores escojan la plataforma más adecuada para su diseño.

Estas nuevas soluciones logran que la incorporación de seguridad basada en hardware sea más sencilla y económica para empresas de cualquier tamaño ya que elimina las barreras asociadas tradicionalmente a la configuración y al abastecimiento de dispositivos.

Esta compañía ha trabajado de la mano con Amazon Web Services (AWS) con el fin de minimizar y agilizar la incorporación de servicios IoT de AWS para los productos diseñados con todas las versiones de la Trust Platform de Microchip.

[39] Interempresas. (10 de Julio de 2019). *Microchip simplifica la seguridad de IoT basada en hardware*. Obtenido de https://www.interempresas.net/Robotica/Articulos/256178-Microchip-simplifica-la-seguridad-de-IoT-basada-en-hardware.html

7. RECOMENDACIONES DE SEGURIDAD PARA IOT

Así como se debe tomar precauciones al momento de conectar un computador, un celular o una Tablet a internet, ya que son propensos a ataques que logran obtener la información que contienen estos dispositivos anteriormente mencionados es necesario adoptar medidas de seguridad para los demás dispositivos que quedan en los hogares pero que al estar conectados a internet se convierten en susceptibles y vulnerables a ataques.

Según el autor Rivas[40], para GB Advisors, líderes en soluciones de Software y Seguridad digital, estas con algunas medidas de seguridad que se pueden tomar para mitigar los riesgos de contar con dispositivos conectados al internet y que estén capturando información personal o hábitos personales.

1. **Realizar un inventario de todos los dispositivos IoT**, de esta manera sabrá exactamente cuáles son los dispositivos y que tipo de información circula a través de ellos.
   Este proceso se puede realizar a través del router principal y así además de tener identificados los dispositivos propios, se podrían identificar si existen dispositivos desconocidos que estén conectados a la red y de los cuales desconozca su proceder.

2. **Realizar test de penetración,** para evaluar el nivel de seguridad tanto de software como de hardware de sus dispositivos.
   Un simple ejercicio es con algún dispositivo externo se puede intentar conectar a cualquier dispositivo IoT que se tenga en el hogar, con las claves que usualmente los fabricante suelen colocarle a los dispositivos y que no se le informa a los consumidores, muchos de los dispositivos no están configurados para solicitar contraseña al momento de conectarse con otro dispositivo.

3. **Analizar los datos,** utilizando diferentes herramientas, puede usar los datos relacionados con el comportamiento de los dispositivos y de esta manera identificar anomalías y tener un rápido poder de reacción ante un ataque.
   Un analizador de tráfico puede ser muy útil para comprender un poco el comportamiento de los dispositivos y sobre todo las conexiones que tienen, con este proceso se puede garantizar que los dispositivos que se tengan no estén realizando conexiones con otros dispositivos ubicados en países con los cuales no deberían tener.

[40] Rivas, G. (20 de Julio de 2018). *El Internet de las Cosas: 5 medidas para garantizar la seguridad del IoT*. Obtenido de https://www.gb-advisors.com/es/iot-seguridad-el-internet-de-las-cosas/

4. **Sistema de cifrado de transporte,** es importante conocer en qué protocolo de comunicación está circulando la información, se debe verificar que utilicen protocolos SSL y TSL para evitar su interceptación en texto plano.
   Otra tecnología que se está implementando para el aseguramiento del internet de las cosas es el Blockchain, que como lo explica Pastorino[41], podría revolucionar el mercado IoT ya que los dispositivos pueden comunicarse a través de la red de manera directa, segura y confiable, sin intermediarios.
   Esta tecnología permite verificar, validar, rastrear y almacenar todo tipo de información, desde certificados digitales, servicios de logística y mensajería, contratos inteligentes y, por supuesto dinero y transacciones financieras.
   Su seguridad radica en que es una tecnología distribuida, donde cada nodo de la red almacena una copia exacta de la cadena, se garantiza la disponibilidad de la información en todo momento. En caso de que un atacante quisiera provocar una denegación de servicio, debería anular todos los nodos de la red, ya que basta con que al menos uno esté operativo para que la información esté disponible.
   La tecnología de blockchain permite almacenar información que nunca se podrá perder, modificar o eliminar

5. **Asegurar la interfaz de la nube,** los usuarios y contraseñas por defecto son el dolor de cabeza para muchos, se debe procurar cambiarlos durante la configuración inicial.
   Es muy importante tener en cuenta que para los dispositivos IoT el primer medio de protección es la contraseña, la cual, la recomendación de muchos expertos es que sea construida los más segura posible, sin embargo a pesar de estas recomendaciones según la revista digital ComputerHoy[42], éstas son las contraseñas más utilizadas por los dispositivos IoT, como se observa en la figura 5.

[41] Pastorino, C. (4 de Septiembre de 2018). *Blockchain: qué es, cómo funciona y cómo se está usando en el mercado*. Obtenido de https://www.welivesecurity.com/la-es/2018/09/04/blockchain-que-es-como-funciona-y-como-se-esta-usando-en-el-mercado/

[42]Pascual, J. A. (25 de Septiembre de 2016). *Estas son las 10 contraseñas más utilizadas para hackear*. Obtenido de https://computerhoy.com/noticias/hardware/estas-son-10-contrasenas-mas-utilizadas-hackear-51646

Figura 5 Top 10 de las contraseñas más usadas en los dispositivos IoT

Los 10 nombres de usuarios y contraseñas más usados para hackear el Internet de las Cosas

Nombre de usuario	Contraseña
root	admin
admin	root
DUP root	123456
ubnt	12345
access	ubnt
DUP admin	password
test	1234
oracle	test
postgres	qwerty
pi	raspberry

Fuente: https://computerhoy.com/noticias/hardware/estas-son-10-contrasenas-mas-utilizadas-hackear-51646

Las contraseñas fuertes o seguras suelen ser un dolor de cabeza para muchas personas, ya que éstas suelen tener una longitud bastante extensa y unos caracteres bastantes difíciles de recordar en ocasiones, pero la empresa de seguridad Panda[43] ofrece unos trucos bastante útiles para ayudar a los usuarios a recordar estas contraseñas seguras:

1. **A partir de una frase:**
   Debe tener un significado especial para el usuario para que sea fácil de recordar, pero para los demás no tendrá ningún significado en especial, lo ideal es combinar letras, números y símbolos, un ejemplo podría ser; “mi combo de hamburguesa con papas y gaseosa cuesta 20 pesos”, al tomar las primeras letras de cada palabras se tendrá una contraseña segura que para nadie tendrá lógica pero para el usuario que la inventó será fácil de recordar, la nueva contraseña, quedaría así; “**Mcdhcpygc20$**”.

[43] Panda Security. (23 de Febrero de 2016). *10 trucos nemotécnicos para crear contraseñas seguras y fáciles de recordar*. Obtenido de https://www.pandasecurity.com/spain/mediacenter/seguridad/10-trucos-para-crear-contrasenas-seguras/

2. Combinar dos palabras:
Se debe elegir dos palabras de fácil recordación como por ejemplo "**Perros**" y "**Gatos**", el siguiente paso es intercalar las letras de cada palabra, el resultado será "**PGeartrooss**", por ahora no cuenta con ningún carácter numérico ni símbolos, pero en el siguiente paso se mostrará cómo fortalecerla un poco más.

3. Convertir las vocales en números:
Tomando como base la anterior contraseña "**PGeartrooss",** el siguiente paso es cambiar las vocales por el número que más se parece, por ejemplo: A=4, E=3, I=1 y O=0, en ese orden de ideas la nueva contraseña quedará así: "**PG34rtr00ss",** aumentando la dificultad para quien intente descifrarla.

4. Sin vocales:
Para confundir un poco más a los atacantes, se podrían eliminar por completo las vocales y dejar solo las consonantes del ejemplo anterior, pasando de esta contraseña, **"PG34rtr00ss"** a esta otra, **"PGrtrss"**, si se adicionan un símbolo y números nuevos será prácticamente indescifrable.

5. El truco del teclado:
Nuevamente se utiliza el teclado, pero en esta oportunidad se reemplazan los números por letras. El primer paso, es seleccionar una secuencia de números que sea fácil de recordar (por ejemplo, algunos números de la identificación). Para este ejemplo usaremos el 25821. El siguiente paso es buscar cada uno de los números en el teclado y presionarlos seguidos por las letras que se encuentran debajo: "2wsx5tgbik8wsx1qaz". Si se desea aumentar la complejidad de la contraseña un poco más, se puede cambiar alguno de los caracteres por símbolos (se puede usar el símbolo que comparta con el numero seleccionado) e incluir alguna que otra mayúscula.

6. Una palabra y números mezclados:
Es fácil, pero se deben elegir palabras y números que tengan la misma cantidad de caracteres para que sea un poco más fácil el proceso de creación, como por ejemplo utilizar "Bigote" y 25821. La clave está en ir escribiendo las letras una por una, mezclando los números pero a la inversa. Quedará así: "**B1i2g8o5t2e**". Por ultimo agregar un símbolo para aumentar su complejidad.

7. Camuflarse con el medio:
Una terrible idea es utilizar una sola contraseña para varios servicios, o aplicaciones, pero un sencillo tip puede convertir una simple contraseña en una segura sin necesidad de tener que memorizar varios términos. Por ejemplo, si se desea registrarse en Facebook, Incluir las letras **"FB"** al inicio o al finalizar la contraseña, si se aplica al primer ejemplo quedaría así: **"Mcdhcpygc20$_FB"**, o podría ser de esta otra forma: **"F4c3b00k_ Mcdhcpygc20$"**.

8. Utilizar un dado y un grupo de palabras:
Este truco es muy popular y es reconocido como el método Diceware[44], se utilizar para construir contraseñas o claves completamente aleatorias y, por ende, muy complejas o seguras, el truco consiste en lanzar un dado y una lista de palabras.

9. Utilizar como guía el Sudoku:
Se debe utilizar papel y lápiz, dibujar una cuadrícula de 6x6, al interior de cada cuadro escribir números al azar. Posteriormente pensar en un patrón como el que se usa habitualmente para desbloquear el dispositivo móvil, un gesto con el dedo sobre esa especie de **sudoku** que acabas de plasmar (por cierto, sería recomendable utilizar uno ya resuelto). Los números por los que pasa tu trazado serán la contraseña o, es decir, el punto de inicio. Para finalizar se puede aplicar alguno de los otros consejos para introducir letras minúsculas y mayúsculas y símbolos. Para muchos este podría ser el mejor sistema de toda la lista. ¿Por qué? Porque si se cambia las números que se han puesto en las casillas (o se utilizar otro sudoku terminado), el mismo trazado te proporcionará una nueva contraseña. Si se recuerda el patrón y las modificaciones, se tendrá contraseñas ilimitadas.

Figura 6. Cuadricula de Sudoku

8	3	5	4	1	6	9	2	7
2	9	6	8	5	7	4	3	1
4	1	7	2	9	3	6	5	8
5	6	9	1	3	4	7	8	2
1	2	3	6	7	8	5	4	9
7	4	8	5	2	9	1	6	3
6	5	2	7	8	1	3	9	4
9	8	1	3	4	5	2	7	6
3	7	4	9	6	2	8	1	5

Fuente: https://www.pandasecurity.com/spain/mediacenter/seguridad/10-trucos-para-crear-contrasenas-seguras/

10. Ultimo consejo: No hacer lo mismo que los demás:

[44] *Diceware. (2003). Diceware en Español. Obtenido de http://world.std.com/~reinhold/diceware_en_espanolA.htm*

Algunos atacantes no solo son muy inteligentes, lo que sucede ese destinan muchas tiempo a pensar en cómo conseguir contraseñas. Es posible que conozcan todos estos métodos, y su efectividad depende de lo bien que se combinen entre sí y de las palabras o números que se utilicen como punto inicial. Se debe aplicar la imaginación. Cualquier cambio sobre lo convencional o sobre lo que hacen la mayoria, puede marcar la diferencia.

Otros expertos como Internet Security ofrecen consejos de seguridad para los consumidores y de esta manera mejorar la seguridad y privacidad de los dispositivos IoT, estos consejos han sido recopilados por el sitio web de negocios y tecnología Ebizlatam[45], en su artículo denominado, "Consejos para mejorar la seguridad y privacidad de IoT", dichos consejos se presentan a continuación.

1. **Tomarse un tiempo antes de comprar**

   Antes de realizar una inversión en un dispositivo que pueda conectarse a internet, no solo se debe indagar sobre las funcionalidades del producto si no también acerca de la seguridad del dispositivo, que tipo de conexiones realiza y que datos recopila.

   Los acuerdos de privacidad en estos dispositivos son muy importantes, ya que se debe tener claro a quienes podría enviarse datos sensibles, como por ejemplo si se contemplara enviar datos de los hijos a algunos anunciantes o terceros.

   Verifique que el dispositivo se pueda actualizar y que estas actualizaciones estén soportadas por fabricantes de renombre.

2. **Actualizar de manera periódica los dispositivos y aplicaciones**

   Se debe verificar si el dispositivo cuenta con la opción de realizar las actualizaciones de manera automática, si es así, se debe activar, ya que de esta forma se garantiza que siempre se cuente con las actualizaciones o parches de mejora que son lanzadas por los fabricantes y libra al consumidor de realizar este proceso que podría no llevarse a cabo por el tiempo que puede tomar, por descuido o por desconocimiento.

3. **Revisar la característica de cifrado**

   Algunos dispositivos cuentan con la capacidad de utilizar el cifrado, pero en algunos dispositivos no lo aplican por defecto, haciendo una similitud con otro elemento de seguridad, sería como contar con una caja fuerte en casa pero dejarla sin seguro, si no se está seguro si su dispositivo cuenta con esta característica o si ya se encuentra activa, se debe consultar el manual de uso o contactar con el soporte técnico del fabricante.

[45] Ebizlatam. (1 de Agosto de 2018). *Consejos para mejorar la seguridad y privacidad de IoT*. Obtenido de http://www.ebizlatam.com/consejos-para-mejorar-la-seguridad-y-privacidad-de-iot/

4. Revisar la configuración de privacidad

Antes de dar “Aceptar” a todo lo que aparezca al momento de la configuración inicial, se recomienda revisar en detalle los acuerdos de privacidad ya que es posible que se vaya a compartir más de lo que se espera y lo más importante es saber quién podrá ver los datos.

Cuando sea posible, lo más recomendable es no vincular el dispositivo a las aplicaciones a las cuentas de redes sociales, ya que en muchas ocasiones la información que se comparte podría atentar contra su propia seguridad física, como por ejemplo: si se comparte el recorrido que realiza a diario, algunas personas podrían utilizar esta información para crear patrones de desplazamiento o momentos de ausencia.

5. No reutilice las contraseñas:

Algo tan mencionado en muchos sitios web, es el tema de las contraseñas y la precaución que se debe tener, lo más recomendable en este caso es usar contraseñas seguras (que se forman utilizando números, letras y caracteres especiales y de longitud superior a 8 caracteres).

Uno de los inconvenientes para muchas personas es que se tienen demasiados elementos que requieren de una contraseña para iniciar sesión y recordar la contraseña para cada elemento puede resultar complejo, así que asignan la misma contraseña a todos sus elementos, esta podría ser una mala práctica ya que si una contraseña es robada o descubierta, inmediatamente un atacante podría tener fácilmente acceso a cualquier elemento.

Actualmente existen gestores de contraseñas seguro que son de gran utilidad siempre y cuando se utilicen adecuadamente, siendo de gran ayuda para administrar todas las contraseñas con que se cuente.

6. Desconectar los dispositivos que no estén en uso

Si por algún motivo ya sea laboral o personal debe ausentarse, la recomendación es desconectar de internet o de la corriente eléctrica aquellos dispositivos que no serán utilizados por algún tiempo prolongado, de esta manera se evita una posible intromisión o manipulación remota en la ausencia.

8. ACCIONES O ESTRATEGIAS DE SEGURIDAD A TOMAR PARA EL USO DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS POCO SEGUROS

Como se ha abordado en los diferentes capítulos de este documento aún falta camino que recorrer en el tema de la seguridad en los dispositivos IoT, ya que si bien es cierto que son conocidas muchas amenazas que han suscitado grandes despliegues noticiosos, existen muchas ocultas que no han salido a la luz pública ya sea por no desear que se conozcan o simplemente porque no se han descubiertos los ataques y los compromisos de los dispositivos.

Es claro que día a día se realizan nuevos lanzamientos de productos de uso doméstico e industrial que dentro de sus virtudes está el hecho de poder utilizar el internet como insumo principal para su operación, esto sin duda resulta muy atractivo para los consumidores ya que para algunos el solo hecho de poder conectarlo a internet es suficiente para tomar la decisión de adquirirlo.

El tema de la seguridad en estos dispositivos aún no tiene la fuerza que debería tener, para citar un ejemplo muy común que ocurre en cualquier tienda de electrodomésticos del país; los SmartTV se encuentran exhibidos en grandes espacios, todos proyectando alguna imagen o video para que los consumidores observen las virtudes de la resolución de sus pantallas, cuando un posible comprador se acerca a uno de estos, el vendedor saca su mejor repertorio sobre su producto, se mencionan la calidad de la imagen (HD, Full HD, 4K, etc.), la potencia de su sonido en Watts, los puertos de conexión que tiene (USB, HDMI, VGA, etc.), pero se quedan cortos al momento de mencionar las conexiones directas que tiene el televisor, solo se limitan a decir que lo puede conectar a internet para ver películas y series, descargar aplicaciones, entre otras actividades, pero de seguridad no se menciona ninguna virtud del dispositivo, al parecer por el desconocimiento que el vendedor tiene sobre el tema o simplemente porque al posible cliente no le interesa escuchar que el televisor cuenta con opciones de cifrado, su contraseña deberá ser cambiada constantemente, tendrá que revisar las actualizaciones de seguridad.

Como el tema de la seguridad debe ser abordado tanto como por fabricantes y consumidores, a continuación se detallan unas acciones o estrategias para que los usuarios finales adopten para minimizar los riesgos que tienen los dispositivos, que a lo largo del documento se ha evidenciado que aún falta mucho para considerarlos seguros.

Algunas de estas estrategias han sido recopiladas del sitio web de seguridad Welivesecurity[46], las cuales no requieren que los usuarios tengan avanzados conocimientos en seguridad.

[46] Welivesecurity. (Marzo de 2019). *Smart tv: ¿una puerta trasera en nuestro hogar?* Obtenido de https://www.welivesecurity.com/wp-content/uploads/2019/03/ESET-seguridad-SmartTV.pdf

- Utilizar contraseñas de seguridad seguras, no repetirlas entre los diferentes dispositivos y en lo posible usar el doble factor de autenticación.

- Cambiar las contraseñas que vienen por defecto de los dispositivos ya que es lo primero que realizan los atacantes, buscar vulnerar dispositivos que cuenten con la contraseña por defecto ya que estas se encuentran fácilmente en internet.

- Utilizar solo las tiendas oficiales para la descarga de las aplicaciones para evitar en gran medida la infección de código malicioso.

- Antes de instalar las aplicaciones leer los comentarios, las valoraciones que tiene y si los permisos que se requiere van acorde a la funcionalidad de la aplicación y si es necesario bloquea los que se consideren potencialmente peligrosos.

- Utilizar redes conocidas y privadas en la medida de lo posible usar solo las redes que hayan sido diseñadas por el propio usuario.

- Estar siempre alerta a los mensajes recibidos por correo electrónico o redes sociales de remitentes desconocidos que contengan enlaces o archivos que no se hayan solicitado, se debe sospechar principalmente de mensajes con asuntos alarmantes o promociones fuera de lo normal.

- Al navegar en internet a través de estos dispositivos y suministrar datos privados, verificar que el sitio cuente con un ciframiento HTTPS o el candado verde.

- Antes de realizar compras en internet verificar muy bien todo el sitio web, que no tenga ningún error de ortografía ya que podría tratarse de una plantilla diseñada para simular el sitio de compras y capturar información confidencial y que su ingreso no sea a través de enlaces, se debe digitar su dirección completa en el navegador.

- Revisar muy bien la información que va a ser compartida en internet, mientras menos información sea compartida menos posibilidades tiene de ser comprometida por algún dispositivo vulnerable.

- Si en algún momento se desea reemplazar algún dispositivo que se tenga conectado a internet y éste se desee vender o donar, se debe verificar que se borre completamente la información para que no pueda ser accedida por ninguna persona no autorizada.

Es necesario recalcar que la protección no solo se logra a través de la instalación de una solución de seguridad, sino también a través de la concientización de los usuarios y sobre todo la adopción de un comportamiento seguro con respecto a las amenazas informáticas.

Para complementar las estrategias entregadas por Welivesecurity, es importante también tener en cuenta las entregadas por SecureWeek[47] en su portal, "6 capas de seguridad que necesita su configuración de IoT", el cual a partir de un análisis enfoca la seguridad en IoT en diferentes capas que deben asegurarse para evitar estar inmerso en un ataque ya sea directo o que alguno de los elementos que podrían ser sea usados para complementar cualquier ataque sin que sea percibido, las capas a las cuales hace referencia SecureWeek para fortalecer la seguridad IoT, son las siguientes:

1. **Seguridad de la red**

   Desafortunadamente, la mayoría de las redes IoT son inalámbricas. Asegurar una red inalámbrica puede ser un poco más complicado, ya que existen diferentes protocolos de comunicación, estándares y capacidades de dispositivos diferentes. Sin embargo, una de las formas más fáciles de proteger una red inalámbrica es cambiar los nombres de usuario y las contraseñas que vienen por defecto en los routers o Access point

   En estos dispositivos generalmente vienen con una página web embebida, como usuario administrador, puede cambiar el nombre de usuario y la contraseña para mantener su red segura. También se debe cambiar el identificador de conjunto de servicios (SSID) predeterminado. Un SSID predeterminado indica una red mal configurada, lo que aumenta las posibilidades de un ataque.

   Cabe recordar que un SSID[48], Se trata de un parámetro propio de los routers, más específicamente el "nombre" de la red inalámbrica. Es el "**identificador de paquetes de servicio**". Esto quiere decir que, cuando un paquete es enviado, es acompañado por esta información para saber en todo momento cuál es la red origen. Cuando el dispositivo se conecta a una red inalámbrica, el SSID pasa a ser compartido, para ocultar esta información se debe ingresar a la configuración web del router y buscar la sección inalámbrica.

2. **Autenticación**

   Este proceso evita que personas no autorizadas obtengan acceso a la red, mientras que le permite al administrador, acceder a las fuentes que necesita. Se

[47] Secure Week. (Marzo de 2019). *6 capas de seguridad que necesita su configuración de IoT*. Obtenido de https://www.secureweek.com/6-capas-de-seguridad-que-necesita-su-configuracion-de-iot/

[48] Crespo, A. (24 de Abril de 2018). *Cómo cambiar el SSID o nombre de nuestra red WiFi*. Obtenido de https://www.redeszone.net/2018/04/24/ssid-red-wi-fi-modificacion/

debe considerar diferentes factores de autenticación. Por ejemplo, es posible que desee permitir que varios usuarios accedan a un dispositivo en particular.

Una autenticación simple consiste en configurar a los usuarios un nombre de usuario y una contraseña para acceder a un dispositivo en particular. Sin embargo, existen dispositivos que permiten utilizar métodos avanzados como la autenticación de dos factores y la biométrica.

En los casos de la autenticación de dos factores, después de ingresar un nombre de usuario y una contraseña, los usuarios reciben una contraseña por correo electrónico o mensaje de texto, en los entornos de alta seguridad se combina adicionalmente con firmas digitales o tarjetas inteligentes.

3. Cifrado o Encriptamiento

La mayoría de las redes domésticas Wi-Fi admiten tecnologías de encriptación como WPA y WPA2, entre otras. Sin embargo, éstos no son algoritmos de cifrado muy fuertes. La longitud y la complejidad de la clave o el número de bits en la clave de cifrado determinan el éxito del cifrado de la red.

Las claves de cifrado tienen un ciclo de vida predeterminado. Por lo tanto, se vuelven poco útiles después del determinado período de uso. Por lo tanto, el cifrado de datos de IoT también requiere ser renovado constantemente.

4. La nube

La nube o el internet es una de las principales fuentes de posibles amenazas cibernéticas que pueden acechar la red de IoT. Es en la nube donde se conectan los dispositivos inteligentes y donde se transmiten y almacenan los datos, por tal motivo requiere protección contra los ataques cibernéticos.

El proveedor de servicios de internet es la primera línea de defensa contra los posibles ataques que atenten contra la seguridad de los datos. Es claro que deben proporcionar un entorno de nube seguro. Por lo tanto, se debe elegir un proveedor de servicios con cuidado, en lo posible uno que use prácticas y controles de seguridad avanzados.

5. Gestión del ciclo de vida del dispositivo

En muchas ocasiones se pasa por alto, los dispositivos IoT y sus sistemas se deben mantener actualizados con regularidad. Se debe activar las actualizaciones automáticas para garantizar que todo, incluidos los sistemas operativos, el firmware y el software de aplicación, se mantenga actualizado.

Los atacantes frecuentemente están buscando dispositivos con huecos de seguridad, por lo tanto los fabricantes de dispositivos y proveedores de servicios en la nube crean parches de seguridad para corregirlos. Se debe asegurar que los parches de seguridad estén instalados correctamente.

6. **Interfaz o protección API**

   Generalmente, se utiliza una interfaz de programación de aplicaciones o API para acceder a los dispositivos conectados a la configuración de IoT. La seguridad de la API es fundamental para garantizar que solo los dispositivos autorizados y las aplicaciones se comuniquen entre sí, garantizando así la integridad de los datos.

   Se puede utilizar una herramienta de gestión de API completa. La mayoría de las herramientas pueden automatizar las conexiones entre una API y las aplicaciones.

El aumento agigantado de las redes de IoT ha facilitado las tareas de muchas personas, pero, también ha aumentado el riesgo de robo de información e identidad. Lamentablemente, asegurar una configuración de IoT es más fácil decirlo que hacerlo, dado a su compleja estructura debido a que cuenta con un sin número de dispositivos.

Con la ayuda de estas seis capas de seguridad mencionadas anteriormente ayudarán a protegerse de las amenazas informáticas.

9. DISCUSIONES ENTORNO ANÁLISIS DEL NIVEL DE SEGURIDAD PRESENTE EN LOS DISPOSITIVOS QUE COMPONEN EL INTERNET DE LAS COSAS

La investigación realizada determina que si bien es cierto los dispositivos IoT cuentan con mecanismos propios de seguridad para contener y evitar cualquier ataque cibernético, éstos no son los suficientemente fuertes para repeler la gran cantidad de ataques a los cuales están expuestos a conectarse a internet.

De igual manera estos dispositivos deben sortear múltiples vectores de ataques[49], tales como ataques físicos, cuando se tiene acceso al dispositivo como tal permitiendo su manipulación, ataque a las comunicaciones, siendo este el más común ya que existen múltiples mecanismos de comunicación para estos dispositivos y ataques a los servicios que permiten tener acceso y/o control remoto de los dispositivos para cometer cualquier acto no autorizado.

Las recomendaciones de seguridad[50] son claras para cualquier tipo de dispositivo IoT, a nivel del dispositivo; confiar solo en fabricantes que garanticen niveles mínimos de seguridad, usar dispositivos con el firmware actualizado, cambiar las contraseñas que vienen por defecto.
A nivel de la conectividad, utilizar canales de comunicación seguros (VPN´s o MPLS), utilizar contraseñas seguras y a nivel de aplicación, doble factor de autenticación, usar protocolos de seguridad y contraseñas seguras.

Las recomendaciones de seguridad que se aprecian en el presente análisis, deben ser consideradas por cualquier empresa o persona para mitigar los riesgos inherentes a cualquier dispositivo IoT que esté conectado a internet.

Aún falta camino por recorrer en materia de seguridad para que todos los actores del internet de las cosas, tales como: fabricantes, desarrolladores, consumidores, puedan sentirse medianamente convencidos de que pueden confiar en los dispositivos IoT.

Es necesario que se diseñen estándares de seguridad para IoT, como lo exigen actualmente para otros sectores de la tecnología, esto sería un buen punto de partida para cerrar la brecha que existen actualmente y que aún no se ha explorado mucho por los ciber atacantes, los cuales tienen su mira en grandes infraestructuras pero que si destinaran un mayor enfoque en los dispositivos IoT, tendrían un campo

[49] Siles, R. (Marzo de 2018). *Vectores de ataques del internet de las cosas*. Obtenido de http://www.redseguridad.com/revistas/red/080/74/index.html

[50] IoT Pirata. (4 de Abril de 2019). *Consejos y recomendaciones de seguridad y privavidad para IoT (Internet de las Cosas)*. Obtenido de https://iotpirata.com/consejos-y-recomendaciones-de-seguridad-iot-internet-de-las-cosas/

de acción bastante amplio y con un poder de destrucción bastante amplio, por no encontrar mucha resistencia en estos dispositivos.

Por lo pronto la recomendación es implementar las medidas de seguridad que se presentan en este análisis, y no esperar a que cualquier dispositivos de la red que se posea se vea comprometido en redes zombies de dispositivos IoT o que sin darse cuenta la información personal de la cual debe estar fuera del alcance de personas no autorizadas, esté siendo sustraída sin ningún tipo de control.

10. CONCLUSIONES

La seguridad en el Internet de las cosas aún está en su etapa de maduración ya que no existen regulaciones como si lo hay para otras tecnologías en internet, los fabricantes solo destinan una pequeña parte de su presupuesto para el tema de la seguridad y mucho para la innovación.

Los controles de seguridad que imponen en sus dispositivos aún no están a la altura de las exigencias de las amenazas de la actualidad, algunos dispositivos que se creen tener mecanismos de seguridad no son lo suficientemente fuertes para contener un ataque no muy sofisticado, ya que con un par de contraseñas de las cuales se conoce que algunos dispositivos traen por defecto y que no son obligadas a cambiar desde la configuración del dispositivo, pueden acceder por completo tomando incluso de manera remota dicho dispositivo.

De igual manera los consumidores no advierten del peligro a los cuales se pueden ver expuestos con el solo hecho de conectar cualquiera de estos dispositivos que en años anteriores solo estaban destinados para realizar actividades domésticas.

Aún falta por crear estándares y/o guías tanto para fabricantes como consumidores respecto a la seguridad en los dispositivos IoT.

En los antecedentes de seguridad que se analizaron en el documento cabe anotar que todos han representado pérdidas considerables de dinero, de información, de tiempo e incluso de haberse materializado por completo el hackeo al automóvil Tesla, su hubiese podido presentar pérdidas humanas.

Pero no todo es malo, si bien es cierto que existen problemas de seguridad que de seguro se irán ajustando con el trascurrir de los años, el internet de las cosas ha revolucionado por completo el concepto de cómo se mira el internet, la accesibilidad y la movilidad de la información es cada vez más ágil.

Dependerá de las personas el buen uso que se le dará a toda esta facilidad de conexión y también estará en muchos casos que dependerá exclusivamente de ellos la seguridad de su información.

11. RECOMENDACIONES

Una vez dado a conocer los problemas de seguridad que tienen algunos dispositivos IoT, se hace necesario que se tomen en cuenta las recomendaciones que a lo largo del documento se expusieron tomando como base la opinión de los expertos en materia de seguridad informática.

Pero sobre todo se hace necesario que se tome conciencia y se tome el tiempo que sea necesario para revisar la seguridad de los dispositivos IoT que se vayan a adquirir y sobre todo se revise con cuidado que tipo de información es que se comparte a través del internet, esto con el fin de no exponer información que no sea necesaria.

No se tiene que ser un experto en seguridad para adquirir dispositivos IoT para sentirse seguros de que no se está en riesgo, hoy en día existen muchas empresas que pueden asesorar a cualquier persona en estos temas, y en internet también existe mucha documentación al respecto.

Si se toman en cuenta las recomendaciones o consejos de seguridad expuestos en este documento, se puede tener la certeza que el riesgo que existe en internet se reducirá enormemente y la información personal o de cualquier índole tendrá menor riesgo de ser interceptada.

Es recomendable nunca bajar la guardia en materia de seguridad y sobretodo nunca sentirse confiado de que no pasará nada o que la información que se maneja no es atractiva para nadie.

12. BIBLIOGRAFIA

PEÑA, Milenka. Qué es el Internet de las Cosas y cómo afecta tu vida diaria. [En línea]. (2019). Disponible en: https://es.digitaltrends.com/tendencias/que-es-el-internet-de-las-cosas/

ROUSE, Margaret. Seguridad de internet de las cosas. [En línea]. (2017). Disponible en: https://searchdatacenter.techtarget.com/es/definicion/Seguridad-de-Internet-de-las-Cosas

RIVAS, Genesis. El Internet de las Cosas: 5 medidas para garantizar la seguridad del IoT. [En línea]. (2018). Disponible en: https://www.gb-advisors.com/es/iot-seguridad-el-internet-de-las-cosas/

GEMALTO. Seguridad integrada y en la nube para el Internet de las Cosas. [En línea]. (2017). Disponible en: https://www.gemalto.com/latam/iot/seguridad-en-iot

LA ROTTA, Santiago. Seguridad en internet de las cosas, uno de los mayores problemas en tecnología. [En línea]. (2018). Disponible en: https://www.elespectador.com/tecnologia/seguridad-en-internet-de-las-cosas-uno-de-los-mayores-problemas-en-tecnologia-articulo-741697

CASTRO, Miguel. Internet de las cosas. Privacidad y Seguridad. [En línea]. (2016). Disponible en: https://sinbad2.ujaen.es/sites/default/files/publications/Memoria_0.pdf

HARAN, Juan. 10 principales fallos de seguridad de los dispositivos IoT. [En línea]. (2019). Disponible en: https://www.welivesecurity.com/la-es/2019/01/07/principales-fallos-seguridad-dispositivos-iot/

RODRIGUEZ. Txema. Esto no lo arregla un antivirus: los problemas de seguridad del Internet de las Cosas. [En línea]. (2018). Disponible en: https://www.genbeta.com/seguridad/esto-no-arregla-antivirus-problemas-seguridad-internet-cosas

REUTERS PLUS AND AVAST. La época del Internet de las cosas: 6 formas de protegerse. [En línea]. (2018). Disponible en: https://blog.avast.com/es/la-epoca-del-internet-de-las-cosas-6-formas-de-protegerse

MEDINA. María. La historia detrás del internet de las cosas. [En línea]. (2017). Disponible en: https://www.elespectador.com/tecnologia/la-historia-detras-de-la-internet-de-las-cosas-articulo-716678

SECMOTIC. Internet de las cosas: riesgos y seguridad. [En línea]. (2016). Disponible en: https://secmotic.com/internet-de-las-cosas-seguridad/

THE WASHINGTON POST. The day of the zombie baby monitors: when hackers weaponized the internet of things. [En línea]. (2016). Disponible en: https://www.washingtonpost.com/opinions/the-day-of-the-zombie-baby-monitors-when-hackers-weaponized-the-internet-of-things/2016/10/25/167fdf42-9a1b-11e6-b3c9-f662adaa0048_story.html

KUZIN. Mikhail, SHMELEV. Yaroslav, KUSKOV, Vladimir. Nuevas tendencias en el mundo de las amenazas IoT. [En línea]. (2018). Disponible en: https://securelist.lat/new-trends-in-the-world-of-iot-threats/87948/

PORTALTIC. España fue el objetivo del 80% de los ciberataques a dispositivos IoT en la primera mitad de 2018. [En línea]. (2018). Disponible en: https://www.europapress.es/portaltic/ciberseguridad/noticia-espana-fue-objetivo-80-ciberataques-dispositivos-iot-primera-mitad-2018-20181217175221.html

HARAN. Juan. 10 principales fallos de seguridad de los dispositivos IoT. [En línea]. (2019). Disponible en: https://www.welivesecurity.com/la-es/2019/01/07/principales-fallos-seguridad-dispositivos-iot/

AVTEST. Pruebas para internet de las cosas. [En línea] (2019). Disponible en: https://www.av-test.org/es/internet-of-things/

PEREKALIN. Alex. Como hackeamos la casa inteligente de nuestro jefe. [En línea]. (2019). Disponible en: https://www.kaspersky.es/blog/hacking-things/18770/

KUKSOV. Igor. Como hackear una casa inteligente. [En línea]. (2019). Disponible en: https://www.kaspersky.es/blog/vulnerable-smart-home/18883/

INSTITUTO INTERNACIONAL DE SEGURIDAD CIBERNETICA. Cómo hackear fácilmente su Smart TV: Samsung y LG. [En línea]. Disponible en: https://www.iicybersecurity.com/hackear-smarttv.html

EL MUNDO. Un hacker roba en un casino colándose a través de una pecera. [En línea] (2018). Disponible en: https://www.elmundo.es/tecnologia/2018/04/17/5ad4a14c46163f1f658b4630.html

CENTRO CRIPTOLOGICO NACIONAL. Internet de las cosas. [En línea]. (2017). Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2261-ccn-cert-bp-05-internet-de-las-cosas-1/file.html

OWASP. Internet of Things Project. [En línea]. (2018). Disponible en: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

ARENAS. M. Internet de las cosas: Ciberseguridad. [En línea]. (2016). Disponible en: https://www.owasp.org/images/3/36/IoT_CyberSecurity.pdf

GEMALTO. La seguridad del IoT – Conecte su negocio de manera segura con soluciones integradas y de seguridad en la nube [En línea]. (2019). Disponible en: https://www.gemalto.com/latam/iot/seguridad-en-iot

CSIRT-CV. Seguridad en Internet de las Cosas, Estado de arte. [En Línea]. Disponible en: http://www.csirtcv.gva.es/sites/all/files/downloads/%5BCSIRT-CV%5D%20Informe-Internet_de_las_Cosas.pdf

RAMIRO. Ruben. Recomendaciones de ciberseguridad en IoT. [En línea]. (2018). Disponible en: https://ciberseguridad.blog/recomendaciones-de-ciberseguridad-en-iot/

DIARIO TI. La necesidad de seguridad en los dispositivos iot [En línea]. (2018). Disponible en: https://diarioti.com/opinion-la-necesidad-de-seguridad-en-los-dispositivos-iot/106732

PUENTE. Garcia. Riesgos y retos de ciberseguridad y privacidad en IoT. [En línea]. (2017). Disponible en: https://www.incibe-cert.es/blog/riesgos-y-retos-ciberseguridad-y-privacidad-iot

ROSE. Karen, ELDRIDGE. Scott & CHAPIN. Lyman [En línea]. (2017). Disponible en: https://www.internetsociety.org/es/resources/doc/2015/iot-overview

REDACCION TECNOLOGIA. El Internet de las Cosas se abre espacio en Colombia. [En línea]. (2018). Disponible en: https://www.elheraldo.co/tecnologia/el-internet-de-las-cosas-se-abre-espacio-en-colombia-496312

FERRER. Isabel. La seguridad de Internet de las Cosas precisa un cambio de comportamiento del usuario. [En línea]. (2018). Disponible en: https://elpais.com/tecnologia/2018/10/26/actualidad/1540564357_433476.html

MERELLA. Alessio. Seguridad Informática en dispositivos Iot. [En línea]. (2018). Disponible en: https://apiumhub.com/es/tech-blog-barcelona/seguridad-informatica-en-dispositivos-iot/

Muy Seguridad. (2019). Estos son los dispositivos IoT más atacados por los hackers. Obtenido de: https://www.muyseguridad.net/2019/06/13/estos-son-los-dispositivos-iot-mas-atacados-por-los-hackers/

Centro de Seguridad TIC de la Comunitat Valenciana. (s.f.). Seguridad en Internet de las Cosas, Estado del arte. Obtenido de http://www.csirtcv.gva.es/sites/all/files/downloads/%5BCSIRT-CV%5D%20Informe-Internet_de_las_Cosas.pdf

La Vanguardia. (19 de Junio de 2019). ¿Es necesario usar un antivirus en un televisor inteligente? Obtenido de https://www.lavanguardia.com/tecnologia/20190619/462958797967/smart-tv-antivirus-seguridad-televisor-malware.html

Patel, H. (2017). *IoT necesita una mejor seguridad*. Obtenido de https://www.isaca.org/Journal/archives/2017/Volume-3/Pages/iot-needs-better-security-spanish.aspx?utm_referrer=

Interempresas. (10 de Julio de 2019). *Microchip simplifica la seguridad de IoT basada en hardware*. Obtenido de https://www.interempresas.net/Robotica/Articulos/256178-Microchip-simplifica-la-seguridad-de-IoT-basada-en-hardware.html

Ebizlatam. (1 de Agosto de 2018). *Consejos para mejorar la seguridad y privacidad de IoT*. Obtenido de http://www.ebizlatam.com/consejos-para-mejorar-la-seguridad-y-privacidad-de-iot/

El Confidencial. (21 de Julio de 2014). *'Hackers' chinos logran vulnerar la seguridad del coche Tesla*. Obtenido de https://www.elconfidencial.com/tecnologia/2014-07-21/hackers-chinos-logran-vulnerar-la-seguridad-del-coche-tesla_165313/

Welivesecurity. (Marzo de 2019). Smart tv: ¿una puerta trasera en nuestro hogar? Obtenido de https://www.welivesecurity.com/wp-content/uploads/2019/03/ESET-seguridad-SmartTV.pdf

Sigfox. (28 de Agosto de 2019). Seguridad de IoT: amenazas actuales y cómo superarlas. Obtenido de https://www.wndgroup.io/2019/08/28/seguridad-de-iot-amenazas-actuales-y-como-superarlas-sigfox/

Pastorino, C. (4 de Septiembre de 2018). *Blockchain: qué es, cómo funciona y cómo se está usando en el mercado*. Obtenido de https://www.welivesecurity.com/la-es/2018/09/04/blockchain-que-es-como-funciona-y-como-se-esta-usando-en-el-mercado/

Panda Security. (23 de Febrero de 2016). *10 trucos nemotécnicos para crear contraseñas seguras y fáciles de recordar*. Obtenido de https://www.pandasecurity.com/spain/mediacenter/seguridad/10-trucos-para-crear-contrasenas-seguras/

Diceware. (2003). Diceware en Español. Obtenido de http://world.std.com/~reinhold/diceware_en_espanolA.htm

Crespo, A. (24 de Abril de 2018). *Cómo cambiar el SSID o nombre de nuestra red WiFi*. Obtenido de https://www.redeszone.net/2018/04/24/ssid-red-wi-fi-modificacion/

Secure Week. (Marzo de 2019). *6 capas de seguridad que necesita su configuración de IoT*. Obtenido de https://www.secureweek.com/6-capas-de-seguridad-que-necesita-su-configuracion-de-iot/

Siles, R. (Marzo de 2018). *Vectores de ataques del internet de las cosas*. Obtenido de http://www.redseguridad.com/revistas/red/080/74/index.html

Bartual, Ó. P. (2018). *Análisis y parametrización de la seguridad en sistemas IoT*. Obtenido de https://riunet.upv.es/bitstream/handle/10251/106950/PERERA%20-%20An%C3%A1lisis%20y%20parametrizaci%C3%B3n%20de%20la%20seguridad%20en%20sistemas%20IoT.pdf?sequence=1&isAllowed=y

Rodríguez, F. G. (Abril de 2015). *El Internet de las cosas y las consideraciones de seguridad*. Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/8492/INTERNET%20DE%20LAS%20COSAS%20TESIS%20Y%20CONSIDERACIONES%20DE%20SEGURIDAD%20-%20FINAL.pdf?sequence=1&isAllowed=y

LLerena, C. A. (Octubre de 2018). *Hacking Etico al IoT mediante SDR*. Obtenido de https://repositorio.uta.edu.ec/bitstream/123456789/28812/1/Tesis_%20t1489ec.pdf

Tarquino Murgueito, D. F., & Garcia Garcia, E. S. (Julio de 2017). *Seguridad en internet de las cosas*. Obtenido de https://repositorio.escuelaing.edu.co/bitstream/001/605/1/Tarquino%20Murgueito%2C%20Daniel%20Felipe%20-%202017.pdf

García, L. C. (2014). *Estudio del impacto técnico y económico de la transición de internet al internet de las cosas (iot) para el caso colombiano*. Obtenido de http://bdigital.unal.edu.co/50458/1/Estudio%20T%C3%A9cnico%20y%20Econ%C3%B3mico%20de%20la%20transici%C3%B3n%20de%20Internet%20al%20Internet%20de%20las%20Cosas%20%28IoT%29%20en%20el%20caso%20colombiano.pdf

Internet Society. (Octubre de 2015). *La internet de las cosas - una breve reseña*. Obtenido de https://www.internetsociety.org/wp-content/uploads/2017/09/report-InternetOfThings-20160817-es-1.pdf

Melian, E. (12 de Agosto de 2019). *Microsoft detecta un hackeo masivo en dispositivos con IoT*. Obtenido de https://www.ciberseguridadpyme.es/destacado/microsoft-hackeo-iot/?cn-reloaded=1